SVEUČILIŠTE U RIJECI

POMORSKI FAKULTET U RIJECI

ANA JURAN

SIGURNOST INFORMACIJSKIH SUSTAVA

DIPLOMSKI RAD

Rijeka, 2014.

SVEUČILIŠTE U RIJECI

POMORSKI FAKULTET U RIJECI

SIGURNOST INFORMACIJSKIH SUSTAVA

INFORMATION SYSTEMS SECURITY

DIPLOMSKI RAD

Kolegij: Poslovni informacijski sustavi

Mentor: dr.sc. Edvard Tijan

Student/studentica: Ana Juran

Studijski smjer: Logistika i menadžment u pomorstvu i prometu

JMBAG: 0081124251

Rijeka, rujan 2014.

Student/studentica: Ana Juran
Studijski program: Logistika i menadžment u pomorstvu i prometu
JMBAG: 0081124251

IZJAVA

Kojom izjavljujem da sam diplomski rad s naslovom SIGURNOST INFORMACIJSKIH SUSTAVA izradila samostalno pod mentorstvom prof. dr. sc. Edvarda Tijana .

U radu sam primijenila metodologiju znanstvenoistraživačkog rada i koristila literaturu koja je navedena na kraju diplomskog rada. Tuđe spoznaje, stavove, zaključke, teorije i zakonitosti koje sam izravno ili parafrazirajući navela u diplomskom radu na uobičajen, standardan način citirala sam i povezala s fusnotama i korištenim bibliografskim jedinicama. Rad je pisan u duhu hrvatskoga jezika.

Suglasna sam s objavom diplomskog rada na službenim stranicama.

Studentica

Ana Juran

SAŽETAK

U suvremeno doba važno je prepoznati značaj informacijskih sustava te iste štititi na prikladan način. Budući da su informacije glavni resurs poslovanja logično je da se koriste razni zakoni, institucije, standardi, procedure, pravila te mjere zaštite informacijskih sustava. Kombinacijom svih tih načina zaštite, informacijski sustavi štite se od prijetnji s kojima se poduzeća susreću u suvremeno doba.

Provedenom anketom dobiva se prikaz stanja u Republici Hrvatskoj te informiranosti zaposlenika te ostalih korisnika neke organizacije. Rezultati ankete pokazali su da je zakonska regulativa Republike Hrvatske razvijena, no potrebno je više educirati zaposlenike da bi se na pravilan način štitile informacije.

Ključne riječi: sigurnost, informacijski sustavi, mjere zaštite, upravljanje sigurnošću, zakonska regulativa

SUMMARY

In the contemporary times it is important to notice the significance of information systems and protect them in a convenient way. Since information is the main resource of the business it is logical to use a variety of laws, institutions, standards, procedures, policies and measures for the protection of information systems. The combination of all these possibilities of protection, information systems are protected from various threats of the modern era.

By conducting a survey we obtained the status of the Republic of Croatia and the awareness of employees and other users of the organization. The survey results showed that the Croatian legislation developed, but it is necessary to educate employees in order to properly protect information.

Keywords: security, information systems, protective measures, security management, legislative regulations

SADRŽAJ

1. UVOD

U današnje vrijeme razne organizacije poput vlada, vojske, bolnica, financijskih institucija te privatnih poduzeća posjeduju ogromne količine povjerljivih informacija koje je potrebno zaštititi kako bi se očuvala njihova povjerljivost. Ukoliko se naruši povjerljivost informacija u određenom poduzeću, ono će se naći u teškoj poziciji što se može odraziti na smanjenje dobiti samog poduzeća, narušavanje ugleda te općenito raznih negativnih radnji vezanih uz protok povjerljivih informacija u neadekvatno vrijeme i na neadekvatnom mjestu.

Problem sigurnosti informacijskih sustava javlja se kada se nedovoljno uzmu u obzir pojedine komponente sustava. Tako se u većini slučajeva najveća pažnja prilikom formiranja sigurnosnih sustava pridaje tehničkim mjerama zaštite, dok je faktor korisnika sustava zanemaren. Potrebno je dobro educirati korisnika sustava i omogućiti mu upoznavanje sa tehničkim aspektima zaštite informacijskih sustava, kako bi cjelokupan sustav imao smisao. Bitno je naglasiti kako se visoka i pravilna sigurnost informacijskih sustava postiže jedino pravodobnom implementacijom svih mjera zaštite, odnosno kombinacijom fizičkih, administrativnih i tehničkih mjera uz educirani ljudski kadar.

Cilj ovog rada jest naglasiti važnost pravilnog funckioniranja informacijskih sustava i koliko zapravo sigurnost informacijskih sustava doprinosi poslovanju i uspješnosti poduzeća. U današnje vrijeme premalo se vodi računa o toliko bitnom faktoru zaštite informacija. Živimo u 21. stoljeću gdje se računala sve više razvijaju i cjelokupni sustavi te sigurnost informacijskih sustava prelazi na novu razinu. Više nije dovoljno samo izgraditi sustave zaštite informacija, a ljudski faktor ostaviti na razini prošlog stoljeća. U ovo doba brzih promjena i ubrzanog razvoja novih tehnologija potrebno je sve više obrazovati ljudski kadar te kroz njihovu izobrazbu omogućiti bolje i efikasnije funkcioniranje cijelokupnog sigurnosnog sustava nekog poduzeća. Javlja se potreba za promišljanjem o potencijalnim štetama koje mogu nastati uslijed zloupotrebe informacija, stoga je itekako bitno usmjeriti pažnju na preventivne aktivnosti koje su zadatak upravo sustava informacijske sigurnosti.

1.1. PROBLEM, PREDMET I OBJEKT ISTRAŽIVANJA

Problem istraživanja vezan je uz pitanje nedovoljnog teoretskog pregleda zaštite informacijskih sustava koji predstavlja jedan od temeljnih procesa koje treba provoditi za uspješno poslovanje svake organizacije u današnje vrijeme.

Iz takve problematike definiran je i predmet istraživanja: istražiti i sistematizirati načine zaštite sigurnosti informacijskih sustava i dokazati njihov značaj u poslovnoj praksi. Objekti istraživanja su sigurnost informacija, mjere zaštite sigurnosti informacijskih sustava te zakonska regulativa vezana uz pojam sigurnosti informacijskih sustava.

1.2. RADNA HIPOTEZA

U okviru tako definiranih problema i predmeta istraživanja postavljena je temeljna radna hipoteza: U Republici Hrvatskoj postoji veliki broj zakona, procedura, pravila te ostale regulative kojima se upravlja informacijskom sigurnošću, ali su zaposlenici i dalje nedovoljno educirani, pa se informacije ne štite na prikladan način.

1.3. SVRHA I CILJEVI ISTRAŽIVANJA

Imajući na umu problem i predmet istraživanja, određeni su svrha te ciljevi istraživanja.

Svrha istraživanja je istražiti koje se procedure i kontrole provode te koje se sve mjere zaštite sigurnosti informacijskih sustava koriste u poslovnoj praksi i na koji način pomažu u rješavanju određenih problema u poslovanju suvremenih organizacija.

Cilj istraživanja je znanstvenim metodama dokazati postavljenu hipotezu;. U Republici Hrvatskoj postoji veliki broj zakona, procedura, pravila te ostale regulative kojima se upravlja informacijskom sigurnošću, ali su zaposlenici i dalje nedovoljno educirani, pa se informacije ne štite na visokoj razini.

1.4. ZNANSTVENE METODE

Prilikom razrade tematike, u odgovarajućim kombinacijama koristit će se sljedeće znanstvene metode: metoda indukcije i dedukcije, metoda analize i sinteze, povijesna metoda, metoda deskripcije, te metoda dokazivanja.

1.5. STRUKTURA RADA

Struktura diplomskog rada, s naslovom Sigurnost informacijskih sustava podijeljena je na šest cjelina.

U prvom dijelu, Uvodu, objašnjen je problem, definiran predmet i objekt istraživanja, postavljena temeljna hipoteza, određeni su svrha i ciljevi istraživanja, navedene su znanstvene metode te je objašnjena struktura rada.

Drugi dio ima naslov Općenito o sigurnosti informacijskih sustava. U ovom dijelu biti će naveden pojam i važnost sigurnosti informacijskih sustava, te će biti objašnjeni pojedini pojmovi vezani uz samu sigurnost informacijskih sustava.

Treći dio Zakonska regulativa o sigurnosti informacijskih sustava pregled je najvažnijih normi te zakona Republike Hrvatske koji se koriste kada je riječ o sigurnosti informacijskih sustava.

U četvrtom dijelu, Mjere zaštite informacijskih sustava, opisivati će se sigurnosno pohranjivanje podataka, antivirusna zaštita, tehničke mjere zaštite informacijskih sustava, kriptografija i sl.

Peti dio, Primjeri iz poslovne prakse, sastojati će se od prikupljenih i obrađenih podataka, te na taj način iznesenim zaključcima - koje mjere sigurnosti informacijskih sustava koriste poduzeća i na kojoj razini je sigurnost informacija u Republici Hrvatskoj.

Posljednji, šesti dio, Zaključak, sastojat će se od sinteze i pregleda spoznaja do kojih se došlo prilikom pisanja diplomskog rada.

2. OPĆENITO O SIGURNOSTI INFORMACIJSKIH SUSTAVA

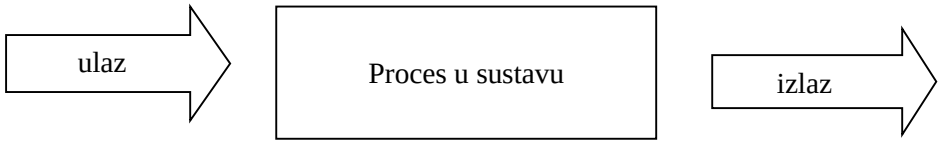
Sigurnost informacijskih sustava vrlo je kompleksan termin, koji je radi lakšeg razumijevanja potrebno raščlaniti na manje dijelove i komponente od kojih se sastoji. Prije nego se krene na razradu tematike sigurnosti informacijskih sustava, potrebno je definirati osnovne pojmove vezane uz sigurnost informacijskih sustava.

2.1. DEFINICIJA SUSTAVA, POSLOVNOG SUSTAVA I NJEGOVOG INFORMACIJSKOG SUSTAVA

Ovisno o kontekstu riječ „sustav“ ima više značenja. Sasvim je logično da primjerice politički sustav i sunčev sustav imaju različito značenje. Iako su različitog značenja, ta dva sustava ali i svaki drugi sustav povezuje zajednička karakteristika, a to je da sustav ne može činiti jedan element. Da bi se nešto nazvalo sustavom potrebno je postojanje niza elemenata koji djeluju sa svrhom postizanja određenog, specifičnog cilja.

Definicija sustava glasi: Sustav je svaki uređeni skup od najmanje dva elementa koji zajedno interakcijom ostvaruju funkciju cjeline[1]. Cilj svakog sustava je zadani ulaz pretvoriti u određeni izlaz. Ovisno o kojoj se vrsti sustava radi, ta pretvorba ulaza u izlaz odvijati će se djelovanjem različitih procesa u sustavu. Ulaz predstavlja skupljene ili dodijeljene veličine koje ulaze u sustav kako bi bile procesirane, odosno kako bi se obradile da bi se dobio željeni izlaz. Proces u sustavu ili obrada ulaznih veličina predstavlja procese transformacije koji konvertiraju ulaz u izlaz, a izlaz predstavljaju transformirane veličine nastale kao produkt procesa transformacije unutar sustava.

Slika 1. Transformacija ulaza u izlaz



Izvor: izradila studentica prema: http://autopoiesis.foi.hr/wiki.php?name=KM+-+Tim+55&parent=NULL&page=Obrada%20podataka (09.05.2014.)

[1] Klasić, K. ; Klarin, K. Informacijski sustavi : načela i praksa. Zagreb : Intus informatika, 2009., str.13

Svaki sustav sastoji se od većeg broja podsustva, a sam sustav često ima svojstva koja nema niti jedan njegov podsustav.

Za razumijevanje tematike ovog rada bitno je nakon definicije sustava odrediti što je to poslovni sustav i što je to informacijski sustav. Poslovni sustav je organizacijski sustav kojeg opisuje skup informacija o prošlosti i sadašnjosti i poslovnih procesa koji ih obrađuju[2]. Poslovni sustav karakteriziraju materijalni ulazi i izlazi te informacijski tokovi pa tako u poslovni sustav ulaze sirovine, dokumenti, poruke, energija, a izlaze dokumenti i proizvodi. Sudionici u procesu pretvorbe ulaza u izlaze mogu biti ljudi kao izvršitelji posla, alati i razni strojevi. Osnova za obavljanje funkcije poslovnog sustava je postojanje informacija. Informacija je podatak obrađen u obliku koji je smislen njezinom primatelju i koji ima stvarnu ili percipiranu vrijednost za njegove sadašnje i buduće odluke i akcije[3]. Informacije su ključni faktor poslovnog sustava jer bez informacija nema ni poslovanja. Iz tog razloga svaki poslovni sustav ima svoj vlastiti informacijski sustav, koji mu služi da se obrađuju podaci o svim segmentima poslovanja.

Informacijski sustav dio je svakog poslovnog sustava, a njegova uloga je konstantna opskrba potrebnim informacijama na svim razinama upravljanja, odlučivanja i svakodnevnog poslovanja. Svako poduzeće ima određenu djelatnost kojom se bavi pa će tako i izgradnja informacijskog sustava za svako poduzeće biti različita. Informacijski sustavi prilagođavaju se i razvijaju za realni poslovni sustav, a poslovni procesi realnog sustava temelj su za modeliranje strukture njegovog informacijskog sustava[4]. Za svaku djelatnost i uspješno poslovanje najvažnije su komponente prikupljanje, obrada i korištenje podataka, pa poduzeće s dobro izgrađenim informacijskim sustavom uspješnije posluje. S obzirom da je već navedeno kako svako poduzeće razvija vlastiti informacijski sustav ovisno o vidu poslovanja, tako taj isti informacijski sustav može, ali i ne mora, biti podržan računalom u cijelosti ili samo određenim segmentima.

Zadaci informacijskog sustava su: prikupljanje, razvrstavanje, obrada, čuvanje, oblikovanje i raspoređivanje podataka svim radnim razinama poslovnog sustava. Ono što je

[2] Klasić, K. ; Klarin, K. Informacijski sustavi : načela i praksa. Zagreb : Intus informatika, 2009., str.16

[3] G. B. Davis, M. H. Olson, Management Information Systems: Conceptual Foundations, Structura andDevelopment, McGraw- Hill, New York, SAD, 1985., str. 200.

[4] http://www.referenceforbusiness.com/management/Comp-De/Data-Processing-and-Data-Management.html, 30.07.2014.

zapravo uloga informacijskog sustava jest proizvesti informaciju na temelju podataka. Podatak je logička cjelina koju primamo osjetilima, a sama za sebe ne mora imati neko značenje. Informacija je skup podataka, a podatak se pretvara u informaciju kada mu je pridruženo neko značenje. Podaci su primjerice: Ana, 22, 01, Pula, 1991. Bilo koji od tih podataka može predstavljati bilo što, primjerice broj 22 može predstavljati 22 kune, 22 godine i tome slično, ali kada mu se prida neko značenje tada postaje informacija. Skup prije navedenih podataka nakon organiziranja i obrade zapravo predstavlja informaciju da je Ana rođena 22.01.1991. godine u Puli. Dakle podatak je činjenica o nečemu iz realnog svijeta, dok je informacija interpretacija podataka koja ima subjektivno značenje za primatelja. Informacijski sustav proizvodi informacije tako da podatke obrađuje, organizira i prikazuje na način koji je razumljiv korisniku, a korisnik tako pripremljene podatke interpretira i na temelju njih donosi odluke u skladu s svojim ovlaštenjima.

Ciljevi informacijskih sustava različiti su za različite radne razine. Najčešća podjela je na tri radne razine: razinu izvođenja (operativnu razinu), razinu upravljanja (taktička razina) i razinu odlučivanja (strateška razina)[5]. Razinu izvođenja karakteriziraju procesi osnovne djelatnosti, a cilj informacijskih sustava na toj razini je povećanje produktivnosti rada. Upravljačka razina odgovorna je za organiziranje, praćenje uspješnosti te otklanjanje smetnji, a cilj informacijskih sustava je povećanje učinkovitosti. Cilj informacijskih sustava na razini odlučivanja jest osiguranje stabilnosti rasta i razvoja s obzirom da je ta razina odgovorna za postavljanje poslovnih ciljeva.

2.2. POVIJEST RAZVOJA INFORMACIJSKIH SUSTAVA

Prva asocijacija na spomen informacijskih sustava jest korištenje računala, međutim poslovni sustavi mogu imati dobro izgrađene informacijske sustave i bez primjene računala. Može se zaključiti kako je informacijski sustav svaki sustav koji se koristi u poslovanju, a zadatak mu je prikupiti, razvrstati, obraditi, čuvati te rasporediti podatke te takav sustav ne mora nužno biti podržan računalom.

2.2.1. Faze obrade podataka

S obzirom na način obrade podataka kroz povijest moguće je odrediti četiri glavne faze. Razvojem informatike usavršavaju se i osuvremenjuju načini obrade podataka

[5] http://ossunist.files.wordpress.com/2013/06/informacijski-sustavi-skripta.pdf, 30.07.2014.

potrebnih u svakodnevnom životu i radu. Iako se govori o povijesnoj distanci te više faza u razvoju načina obrade podataka, neke od njih se i danas primjenjuju.

Povijesne faze obrade podataka su[6]:

1. Faza ručne obrade podataka. U ovoj fazi za obradu podataka primjenjuje se rad ruku, medij za pohranu podataka i dostupni alati za pisanje po tom mediju. Medij je bio primjerice kamen na koji su se urezivali simboli, zatim papirus na kojem se pisalo trstikom, glinene pločice, te papir. Fazu ručne obrade podataka karakterizira spora obrada podataka, obrađuje se relativno mala količina podataka, a sama obrada je bila nepouzdana i upitne točnosti. Kako bi se nadoknadila niska produktivnost upotrebljavao se veći broj ruku koji su evidentirali podatke.

2. Faza mehaničke obrade podataka. To je faza koja počinje sredinom 17.stoljeća kao posljedica općeg razvoja znanosti i tehnike, a karakterizira ju povećanje produktivnosti, točnosti i količine obrađenih podataka. U to doba poznati matematičari i fizičari konstruirali su prve pomoćne uređaje za obradu podataka. Tako je Blaise Pascal konstruirao uređaj koji se smatra pretečom današnjih analognih računala, a Gottfried Leibniz uređaj koji se smatra pretečom današnjih digitalnih računala[7]. Najveći doprinos u to doba, ne samo razvoju informacijske znanosti već i društvenih odnosa u cjelini, donosi Henry Mill konstrukcijom prvog mehaničkog pisaćeg stroja. Poslovi pisanja na pisaćem stroju postaju jednako cijenjenim i za muškarce i za žene što je ženama omogućiilo dulje i kvalitetnije školovanje, a kao završene tipkačice mogle su se samostalno uzdržavati.

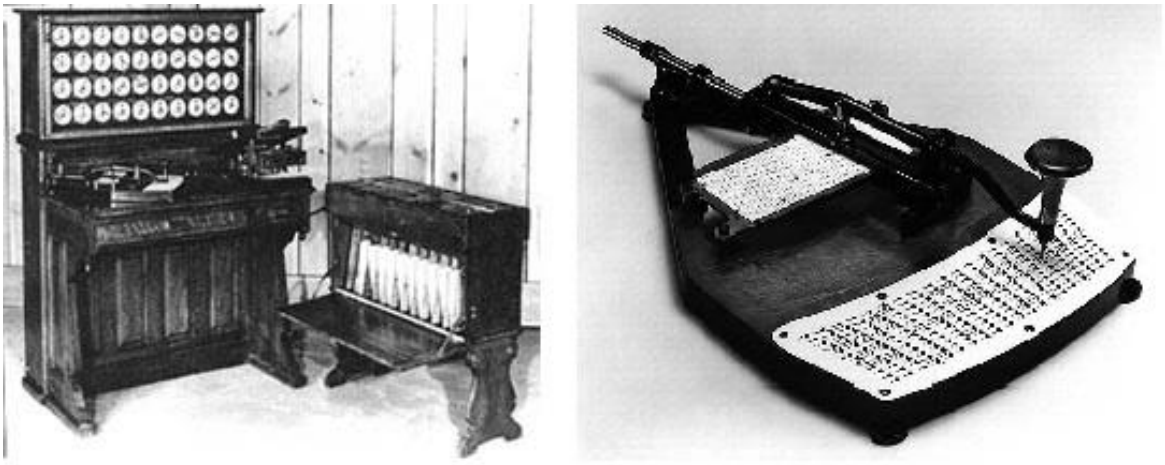
3. Faza elektromehaničke obrade podataka. Ova faza razvija se u drugoj polovici 19.stoljeća, kada je vlada SAD-a raspisala javni natječaj za konstruiranje uređaja kojim bi se podaci popisa stanovništva mogli obraditi u što kraćem roku. Ova faza u literaturi često se naziva i fazom kartične, mehanografske ili birotehničke obrade podataka. Razlog tomu je pobjeda Hermanna Holleritha na raspisanom natječaju s prijedlogom da se kao nositelj podataka koristi bušena kartica, a za njihovu obradu da se upotrijebi poseban elektromehanički stroj. Na slici 2. prikazan je upravo taj

[6] http://www.unizd.hr/portals/1/primjena_rac/brodostrojarstvo/predavanje_1.pdf, 30.07.2014.

[7] http://www.zbrdazdola.com/infobible/infobible/razvoj_racunala_kroz_povijest.htm, 30.07.2014.

elektromehanički stroj odnosno sortirni stroj i bušene kartice koje su se koristile prilikom popisa stanovništva u to doba u SAD-u.

Slika 2. Sortirni stroj i bušene kartice



Izvor: Izrada studentice prema: http://www.columbia.edu/cu/computinghistory/census-tabulator.html, 10.05.2014.

Doprinosom Hermanna Holleritha omogućena je masovna obrada velike količine podataka, a Hollerith se obogatio i osnovao tvrtku iz koje se 1924.godine razvio IBM.

4. Faza elektroničke obrade podataka. Ta faza počinje razvojem ENIAC-a 1944.godine. ENIAC se smatra prvim pravim elektroničkim računalom[8]. Karakteristike ove faze su zanemariv broj grešaka te iznimno velike brzine obrade velike količine podataka. Omogućeno je trajno i privremeno pohranjivanje podataka te povezivanje operacija nad podacima kao što je obrada i prijenos podataka, integracija obrade teksta, grafika, slika i zvuka. Danas najrasprostranjeniji način obrade podataka svakako je internet, koji također spada u ovu fazu.

2.2.2. Faktori uvođenja informatizacije poslovanja

Iako korištenje računala i računalom podržanih informacijskih sustava u mnogočemu olakšava svakodnevno poslovanje, manja poduzeća i danas često dio poslova obrade podataka rade ručno. Postoji nekoliko kriterija koji utječu na odluku da li će se primjenjivati računalo i računalom podržani informacijski sustavi, a oni su: velika količina podataka, pad

[8] http://www.linfo.org/eniac.html, 30.07.2014.

cijene materijalno-tehničke komponente, kvaliteta i mogućnosti nematerijalne komponente informacijskih sustava, informacijska zrelost ljudskih resursa, razvoj i dostupnost sredstava i veza za prijenos podataka i komunikaciju, te organizacijska zrelost poslovnog sustava[9].

Najznačajniji kriterij za donošenje odluke o informatizaciji poslovanja je velika količina podataka koju je potrebno pohranjivati i obrađivati. Ako se radi o manjem broju podataka lakše je i jednostavnije i često jeftinije obraditi podatke ručno, no ako se radi o velikoj količini podataka tada će proces obrade biti jednostavniji i točniji ukoliko se primjeni odgovarajući računalni program.

Pad cijene hardware-a odnosno materijalno-tehničke komponente dovodi do toga da računala postaju dostupna kako poduzećima tako i privatnim osobama. Iz tog razloga mnoga poduzeća odlučuju se na kupnju informatičke opreme odmah na početku rada, a poduzeća koja posluju duži niz godina nešto sporije se odlučuju na obnovu i kupnju informatičke opreme.

Od velike važnosti za donošenje odluke o informatizaciji poslovanja je kvaliteta i mogućnosti nematerijalne komponente informacijskih sustava, odnosno software-a. Informatizaciji poslovanja mnogobrojnih tvrtki u velikoj mjeri doprinosi mogućnost gotovih programskih rješenja koji se na tržištu kupuju po relativno jeftinoj cijeni, ali još više tomu pridonosi mogućnost razvoja tj. prilagodbe softvera po mjeri.

Informacijska zrelost ljudskih resursa faktor je od presudne važnosti za uvođenje informatizacije poslovanja u nekoj tvrtki[10]. Može se dogoditi da je tvrtka opremljena sa najsuvremenijim hardverom i softverom, no zaposlenici nisu dovoljno obrazovani ili iz bilo kojih drugih razloga nisu sposobni raditi u tako postavljenim uvjetima, te odbijaju raditi na računalima usporavajući poslovanje na taj način. U današnje vrijeme poznavanje rada na računalu postaje jedan od uvjeta pri zapošljavanju, te se potiče informatizacija poslovanja.

Razvoj i dostupnost sredstava i veza za prijenos podataka i komunikaciju omogućilo je širenje tržišta za usluge i proizvode poduzeća, te bolju povezanost unutar samog poduzeća, ali i njegovu povezanost s okolinom. Taj razvoj među ostalim omogućio je i rad od kuće te

---

[9] Klasić, K. ; Klarin, K. Informacijski sustavi : načela i praksa. Zagreb : Intus informatika, 2009., str.21

[10] http://www.promeng.eu/downloads/training-materials/ebooks/business-information-systems.pdf, 30.07.2014.

na daljinu, veću fleksibilnost radnog vremena, a samim time i tzv. rad od jutra do noći. Utjecaj komunikacijskih tehnologija veliki značaj ima pri formiranju novih usluga i prilikom otvaranja novih radnih mjesta na poslovima računalima podržanog poslovanja. U prvom redu to se odnosi na povezivanje poduzeća s poslovnim bankama i plaćanje putem interneta, zatim prodaja proizvoda putem interneta i slično. Primjer takve vrste poslovanja su tvrtke eBay i Amazon.

Organizacijska zrelost poslovnog sustava je poveznica prije navedenih kriterija. Ona predstavlja sve mjere, metode i propise kojima se usklađuje njihov rad. Upravo zato što ovaj kriterij prožima sve kriterije može se zaključiti da bez dobre organizacije poslovanja, nema ni dobre informatizacije poslovanja. Ako se radi o lošoj organizaciji i informatizaciji poslovanja, uvođenje računala neće odmah riješiti probleme jer se informacijski sustavi na kraju krajeva grade na temelju pravila koja postoje ili ne postoje u poslovnom sustavu ali uvođenje informacijskih sustava podržanih računalom utječe na organizacijsku zrelost tvrtke te dugoročno uvodi red u organizacijski kaos[11].

Na samom začetku informatizacije poslovanja prva računala bila su iznimno skupa, ali budući da je njihovo svojstvo bilo od državne važnosti najprije su se razvili vojni sustavi. Nakon toga uslijedila je informatizacija knjigovodstva i računovodstva s obzirom da je razvojem programske podrške omogućeno da se jeftinije, brže i točnije obrade velike količine podataka prema jasnim i definiranim pravilima. Bez obzira što je računalna podrška bila potrebna i drugim segmentima poslovanja, najčešće su članovi poslovodstva poduzeća zaduženi za financijske poslove kupovali skupe programe i računala. Idući korak bila je podrška kadrovskoj operativi, najčešće u obliku programa za obračun plaća. Tek nakon što je izvedena podrška za te vidove poslovanja započela je primjena računala za podršku proizvodnji. Proizvodni procesi su mnogo složeniji, razlikuju se ovisno o vrsti proizvodnje i teže ih je implementirati. Programska podrška poslovodstvu posljedenja je uvedena u primjenu u društvu, ali za sada samo u veoma malom broju poduzeća.

2.3. VRSTE INFORMACIJSKIH SUSTAVA

Mnogo je kriterija za podjelu informacijskih kriterija, a oni najčešće korišteni su podjela prema konceptualnom ustrojstvu poslovodstva, prema namjeni ili prema modelu poslovnih funkcija u poslovnom sustavu.

[11] http://ossunist.files.wordpress.com/2013/06/informacijski-sustavi-skripta.pdf, 30.07.2014.

2.3.1. Informacijski sustavi prema konceptualnom ustrojstvu poslovodstva

Kada je riječ o razinama upravljanja u organizacijskom sustavu dijelimo ih na operativnu, taktičku i stratešku razinu. Logično je da se informacijski sustavi razlikuju po razinama, upravo zato jer svaka razina ima drugačije nadležnosti i zadatke. Na tablici 1. prikazane su vrste informacijskih sustava prema konceptualnom ustrojstvu poduzeća.

Tablica 1. Vrste informacijskih sustava prema konceptualnom ustrojstvu poslovodstva

Ustroj poslovodstva		**Vrste informacijskog sustava**	
Poslovodsto	*Strateški nivo*	Odlučivanje	**Sustav potpore odlučivanju**
Izvršno vodstvo	*Taktički nivo*	Upravljanje	**Izvršni informacijski sustavi**
Operativno vodstvo	*Operativni nivo*	Izvođenje	**Transakcijski sustavi**

Izvor: izrada studentice prema: Klarin, Klasić, 2009, str.23

Prema konceptualnom ustrojstvu poslovodstva transakcijski sustavi su vrsta informacijskih sustava namjenjena operativnoj razini, a njihova uloga je izvođenje procesa osnovne djelatnosti. Primjerice to može biti sustav kojim se evidentiraju pojedini koraci u proizvodnji. Kao rezultat izvršnog informacijskog sustava dobivaju se izvješća nužna za upravljanje i ona se pridružuju taktičkoj razini poslovanja. Informacijski sustav strateške razine poslovanja jest sustav potpore odlučivanju.

2.3.2. Informacijski sustavi prema namjeni

Prema namjeni informacijske sustave možemo podijeliti na četiri podsustava, a to su: sustavi za obradu podataka, sustavi podrške uredskom radu, sustavi podrške u odlučivanju i ekspertni sustavi[12].

Sustavi obrade podataka koriste se kako bi se unesli, obradili i pohranili podaci o stanju sustava i poslovnim događajima. Podaci u ovim informacijskim sustavima pohranjuju se u bazama podataka, a do traženih podataka u bazi dolazi se uz pomoć posebnih programa za pretraživanje. Kada se podaci obrade, na temelju njih izrađuju se posebna izvješća čija je svrha pravilno izvođenje procesa osnovne djelatnosti, ali isto tako služe za upravljanje.

[12] Klasić, K. ; Klarin, K. Informacijski sustavi : načela i praksa. Zagreb : Intus informatika, 2009., str.23

Sustavi podrške uredskom radu dijele se u dvije kategorije. Razlikujemo sustave za podršku ljudskog komuniciranja za čiju podršku se koriste elektronička pošta, telefoniranje i slično, te drugu vrstu sustava, sustav za podršku u obavljanju administrativnih poslova. Ovaj sustav korisit pomoćni sustav za potporu rada u skupini, prezentacije i sl.

Kod sustava podrške u odlučivanju primjenjuju se razni modeli odlučivanja pomoću kojih se stvaraju informacije potrebne za odlučivanje, kao podrška pojedincu i grupi.

Kao podrška stručnjacima i ekspertima za rješavanje problema poput konfiguriranja i dijagnosticiranja koriste se ekspertni sustavi. U kategoriju ekspertnih sustava mogu se ubrojati i sustavi podrške posebnim problemskim područjima, a koji se odnose na podršku učenju, podršku znanstvenom i stručnom radu ili podršku projektiranju.

Usporednim prikazom važnijih obilježja različitih vrsta informacijskih sustava prema namjeni dobiti će se slika o složenosti pojedine kategorije. Uzme li se primjerice područje primjene može se primjetiti kako su neki informacijski sustavi složeniji od drugih. Pa su tako obilježja sustava obrade podataka dobro struktuirana problemska područja čiji se procesi mogu strukturalno pratiti. Kod sustava uredskog poslovanja obilježja su dobro strukturirani ponavljajući uredski poslovi, a sustavi podrške odlučivanju obilježeni su djelomičnim strukturiranim procesima donošenja odluka. Najsloženije područje primjene je kod ekspertnih sustava čije su obilježje uska problemska područja za koja su potrebna ekspertna znanja. Skladište podataka i informacija također se razlikuje ovisno o informacijskom sustavu. Sustavi obrade podataka imaju baze podataka organizacijskog sustava, sustavi uredskog poslovanja imaju baze podataka pojedinih programskih pomagala te baze podataka o objektima, sustavi podrške odlučivanju koriste se bazama izdvojenih podataka, bazama vlastitih podataka, bazama podataka sa rezultatima obrada te bazama modela, u konačnici ekspertni sustavi koriste baze znanja[13]. Svaki od četiri informacijska sustava ima i različitu vrstu i oblik izlaznih informacija, pa tako govorimo li o sustavima obrade podataka oni prikazuju informacije putem analitičkih i zbirnih izvješća, izvješća o greškama i porukama, te informacijama o stanjima i promjenama stanja pojedinih objekata. Sustavi uredskog poslovanja izlazne informacije prikazuju sadržajem poruka, dokumenata i ostalih objekata, a prikazuju i informacije o stanjima i promjenama pojedinih objekata uredskog sustava. Složenost u prikazu izlaznih informacija vidi se u sustavima podrške odlučivanju gdje su gradički, numerički i tekstualno prikazane informacije potrebne za donošenje odluka, a

[13] http://hr.wikipedia.org/wiki/Informacijski_sustavi, 30.07.2014.

informacije su međurezultati obrada. Četvrta vrsta informacijskih sustava, ekspertni sustavi prikazuju izlazne informacije u obliku rezultata ekspertize s objašnjenjima, te ih karakterizira prikaz načina rješavanja problema.

2.3.3. Informacijski sustavi prema modelu poslovnih funkcija u poslovnom sustavu

Treća kategorizacija informacijskih sustava je ona prema modelu poslovnih funkcija u poslovnom sustavu. Kada je riječ o takvoj kategorizaciji informacijskih sustava, oni će biti u tolikom broju koliko se poslovnih funkcija obavlja u poduzeću, dakle ovise o organizaciji poslovanja. Općenito podjela informacijskih sutava prema modelu poslovnih funkcija u poslovnom sustavu je sljedeća[14] :

- Informacijski podsustav (IPS) planiranja i analize poslovanja
- IPS upravljanja trajnim proizvodnim dobrima
- IPS upravljanja ljudskim resursima
- IPS upravljanja financijama
- IPS nabave materijala i sirovina
- IPS prodaje proizvoda i usluga
- IPS računovodstva
- IPS istraživanja i razvoja itd.

Budući da različiti poslovni sustavi imaju različit značaj primjene informacijske tehnologije, informacijske sustave može se podijeliti na četiri osnovna tipa: operativni informacijski sustav, potporni informacijski sustav, strateški informacijski sustava te izgledni informacijski sustav.

Uspjeh tekućeg poslovanja ponajprije ovisi o operativnom informacijskom sustavu. U takvom sustavu informacijski sustav služi kao potpora svakodnevnom poslu pa samim tim i

[14] Klasić, K. ; Klarin, K. Informacijski sustavi : načela i praksa. Zagreb : Intus informatika, 2009., str.25

funkcioniranje poduzeća ovisi o danoj informacijskoj tehnologiji. Primjer gdje se koristi operativni informacijski sustav jest trgovina.

Potporni informacijski sustav nije od velike važnosti za poslovni uspjeh poduzeća ali svakako je koristan. U takvom sustavu vrlo je mala ovisnost informacijske tehnologije, te i bez nje poduzeće funkcionira sasvim solidno. Primjerice u građevinarstvu se koristi potporni informacijski sustav.

Strateški informacijski sustav od velike je važnosti za budućnost poslovanja te za poslovnu strategiju stoga je potrebno da takav sustav omogućava pohranu i brzu obradu velike količine podataka potrebnih za poslovanje[15]. Kada je riječ o takvoj vrsti poslovanja funkcioniranje poduzeća jako ovisi o primjeni informacijske tehnologije, kao i na sami poslovni rezultat poduzeća. Primjer gdje se koriste strateški informacijski sustavi je rezervacija karata za prijevoz putnika.

Izgledni informacijski sustav mogao bi utjecati na uspjeh budućeg poslovanja, pa se može reći da je ovisnost funkcioniranja poduzeća o informacijskoj tehnologiji mala, ali je utjecaj informatike na poslovni rezultat velik. Primjenu ove vrste informacijskog sustava najlakše je prikazati na primjeru osigurateljske djelatnosti. Dakle osiguratelj može ručno izdati policu osiguranja ili obraditi štetu, ali kada je riječ o raznim izračunima premije osiguranja ili procjene rizika za određene ciljne skupine, tada je potrebno prikupiti i obraditi veliku količinu podataka. Bez korištenja informatike taj proces trajao bi predugo te bi se odrazio na rezultate poslovanja.

U principu svakom poslovnom sustavu odgovara neki informacijski sustav. Najčešće se informacijski sustavi odabiru prema osnovnoj djelatnosti samog poduzeća, jer se na taj način najlakše određuje redoslijed prioriteta pri uvođenju informacijskih sustava. Često je u poduzećima najjednostavnije najprije izgraditi potporni informacijski sustav koji s vremenom, kako raste poduzeće, prerasta u izgledni informacijski sustav. Izgledni informacijski sustav ključan je za dugoročno poslovanje poduzeća.

Budući da su informacijski sustavi dio poslovnog sustava, upravo je pravilno i uspješno integrirani informacijski sustavi jedna od glavnih komponenti čiji je rezultat uspješno poslovanje poduzeća. Da bi informacijski sustav bio uspješan, neovisno o kojoj vrsti ili tipu se radi, potrebno je da takav sustav ima dovoljne količine kvalitetnih, dobro i jednoznačno

[15] http://ossunist.files.wordpress.com/2013/06/informacijski-sustavi-skripta.pdf, 30.07.2014.

definiranih podataka koje je potrebno obraditi. Bez tako definiranih podataka nema ni kvalitetne podrške klijentima te rasta i razvoja poduzeća.

Postoji nekoliko načela koja kvalitetan informacijski sustav mora zadovoljiti[16]:

- Informacijski sustav je model poslovne tehnologije organizacijskog sustava
- Podaci su resurs poslovnog sustava
- Temelj razmatranja prilikom određivanja podsustava su poslovni procesi kao nepromjenjivi dio određene poslovne tehnologije
- Informacijski sustav izgrađuje se integracijom podsustava na osnovi zajedničkih podataka – modularnost
- Informacije za upravljanje i odlučivanje izvode se na temelju zbivanja na razini izvođenja

Poduzeće koje ima postavljen informacijski sustav na primjeni navedenih načela u potpunosti zadovoljava svoju zadaću, a to je prikupljanje, obrada, pohrana te distribucija podataka svima kojima je to potrebno. Cilj postojanja informacijskog sustava je unaprijediti poslovanje i ostvariti pozitivan poslovan rezultat.

2.4. SIGURNOST I INFORMACIJSKA SIGURNOST

Budući da je tema ovog rada sigurnost informacijskih sustava, uz prije definirane pojmove potrebno je odrediti što je zapravo sigurnost i što je informacijska sigurnost.

2.4.1. Pojam sigurnosti

Sigurnost se može definirati kao proces održavanja prihvatljivog nivoa rizika. To znači da sigurnost nije konačni proizvod ili završno stanje, već proces. Kada je riječ o zaštiti informacijskih sustava i sigurnosti tada postoji nekoliko osnovnih pravila koja i danas važe kao osnovni postulati:

[16] Klasić, K. ; Klarin, K. Informacijski sustavi : načela i praksa. Zagreb : Intus informatika, 2009., str.26

- uz postojanje različitih tehničkih zaštita potrebno je razmotriti i ljudski faktor sa svim svojim slabostima
- potrebno je naglasiti da apsolutna sigurnost ne postoji
- sigurnost je proces, skup usluga, proizvoda ili procedura te raznih drugih elemenata i mjera koje se konstantno provode

Kako bi se omogućilo normalno poslovanje organizacije potrebno je prikladno zaštititi informacije koje se smatraju imovinom svake organizacije. Zahtjev za zaštitom informacija sve je važniji jer u okruženju distribuiranosti poslovne okoline informacije postaju izložene ranjivosti i većem broju prijetnji. Bez obzira u kojem se obliku informacija nalazila vrlo je važno prikladno je zaštititi. Informacije mogu biti zapisane na papiru, pohranjene u elektroničkom obliku, sačuvane na filmu, mogu se prenositi poštom ili elektroničkim putem i sl. Bilo koja od tih oblika informacija u današnje vrijeme predstavlja najvažniji i najskuplji resurs u poslovanju. Upravo tajnost informacija, ispravnost i pravovremeno posjedovanje daju organizaciji moć ka napredku.

2.4.2. Informacijska sigurnost

Informacijska sigurnost je disciplina kojoj je osnovni cilj osigurati zaštitu informacija i informacijskih sustava od neovlaštenog pristupa, korištenja, primjene ili uništavanja[17]. Cilj informacijske sigurnosti svakako je zaštititi informacije od velikog broja prijetnji u svrhu smanjenja poslovnih rizika, osiguranja poslovnog kontinuiteta te u konačnici povećanja broja poslovnih prilika i povrat od investicija. Bitno je naglasiti kako se informacijska sigurnost postiže primjenom raznih kontrola kao što je sigurnosna politika, razni procesi i procedure, no o tome će biti riječi u daljnim poglavljima ovoga rada.

Informacijska sigurnost je važna u današnjem poslovanju, upravo zato jer su informacije, pripadni procesi, sustavi i mreže vrlo važan dio poslovne imovine. Kako bi se osigurao poslovni ugled, zadovoljile zakonske norme te kako bi se osigurao dotok novca, profitabilnost i ostvarila te zadržala konkurentnost od presudne važnosti može biti definiranje, implementacija, održavanje te poboljšanje informacijske sigurnosti. Postoje brojne sigurnosne prijetnje s kojim se organizacije suočavaju poput računalnih prijevara,

[17] Sigurnost informacijskih sustava : priručnik. Zagreb : Algebra, 2010., str. 6

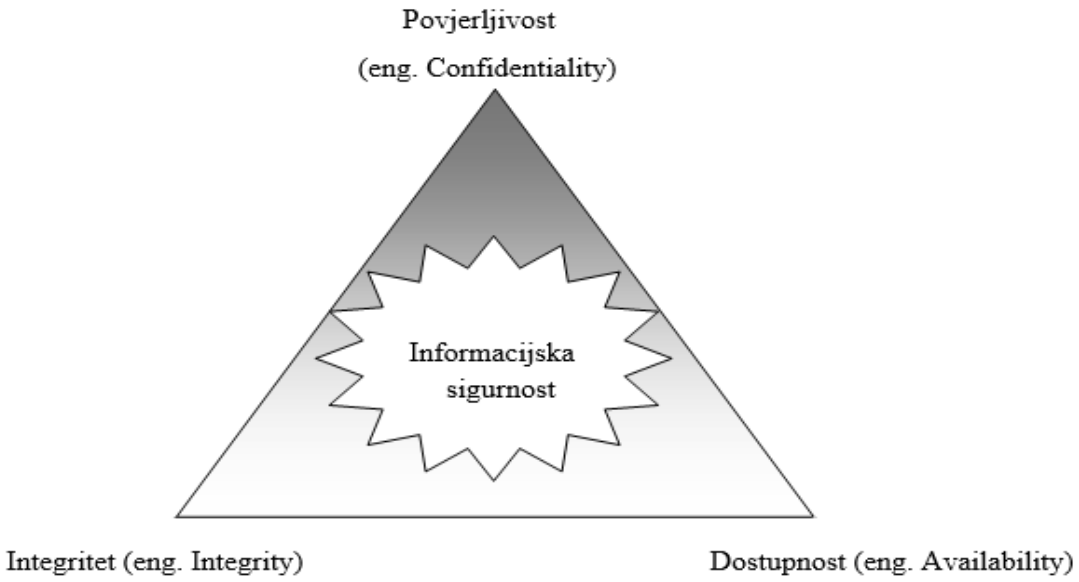
špijunaža, sabotaža, vandalizma, požara, poplava i slično. Sve prisutnije su štete nanesene organizaciji u obliku zloćudnog koda, računalnog hakiranja i uskraćivanja usluge.

Informacijska sigurnost je od jednake važnosti kako za javna tako i za privatna poduzeća. Povezanost javnih i privatnih računalnih mreža i dijeljenje informacija otežavaju kontrolu pristupa informacijama. U takvim uvjetima oblici centralizirane kontrole nisu učinkoviti. Kako bi se pravilno vršilo upravljanje informacijskom sigurnošću zahtjeva potrebno je sudjelovanje svih zaposlenika organizacije, a često je potrebna i pomoć konzultanta izvan granica organizacije.

2.4.3. Aspekti informacijske sigurnosti

Cilj svakog informacijskog sustava je zaštititi informacije od neovlaštenih izmjena, odnosno potrebno je osigurati integritet, zatim je potrebno zaštititi informacije od objavljivanja tajnih informacija što se odnosi na povjerljivost i u konačnici informacije je potrebno osigurati dostupnim ovlaštenim korisnicima[18]. Povezanost ovih tri aspekta prikazana je na Slici 3. kroz osnovni sigurnosni trokut (eng. CIA triad).

Slika 3. Osnovni sigurnosni trokut



Izvor: izrada studentice

[18] http://www.techopedia.com/definition/25830/cia-triad-of-information-security, 30.07.2014.

Prvi i najočitiji aspekt informacijske sigurnosti je povjerljivost podataka. Povjerljivost podrazumijeva u prvom redu tajnost podataka i mogućnost dostupnosti podataka samo ovlaštenim osobama. Svakako kod ovog aspekta najveća pažnja usmjerena je na korisničku identifikaciju i autentifikaciju.

Postoje razne prijetnje što se tiče povjetljivosti podataka, a najčešće su: hakiranje, maskiranje, neovlaštena korisnička aktivnost, nezaštićeno preuzimanje datoteka, lokalne mreže, trojanski konji i sl. Najgrublje rečeno postoje dvije metode zaštite povjerljivosti informacija, a to su korištenje kontrole pristupa (fizičke i logičke) i metoda enkripcije. Kada je riječ o kontroli pristupa vrlo je jednostavno odrediti povjerljivost podataka. Jednostavno osobe koje su ovlaštene za pristup informacijama moći će doći do njih, a ostalim korisnicima pristup tim informacijama je onemogućen. Metoda enkripcije nešto je kompliciranija pa kako bi se pristupilo informacijama, ovlašteni korisnici moraju imati tajni ključ koji im omogućuje uvid u informacije, jer ostali korisnici također mogu imati pristup istim informacijama, ali bez tajnog ključa te informacije su za njih besmisleni podaci.

Drugi aspekt sigurnosnog trokuta je integritet. Pod pojmom integriteta podrazumijeva se činjenica da informacija (podaci) ne mogu biti promijenjeni bez odgovarajućeg ovlaštenja, odnosno da su onemogućene promjene od strane neovlaštenih osoba ili neovlaštene promjene ovlaštenih osoba[19].

Ciljevi integriteta ponajviše se odnose na sprječavanje neovlaštenih korisnika da modificiraju podatke ili programe, zatim sprječavanje ovlaštenih korisnika da modificiraju podatke ili programe na nepropisan i neovlašten nalin i u konačnici održavanje konzistentnosti podataka i programa. Baš kao i povjerljivost, integritet se čuva upotrebom kontrole pristupa i enkripcijskim algoritmom. Način na koji se može vidjeti gubitak integriteta jest u slučaju da neovlašteni korisnik napravi bilo kakve promjene na enkriptiranim podacima informacije koje su enkriptirane u većini slučajeva budu nepovratno izgubljene. Nažalost ako neovlaštenu promjenu napravi osoba koja je ovlaštena za pristup podacima, tada nije tako lako utvrditi gubitak integriteta.

Kao treći aspekt informacijske sigurnosti navodi se dostupnost, a taj pojam odnosi se upravo na dostupnost podataka i informacija. Najviši cilj dostupnosti je osigurati korisnicima

[19] Sigurnost informacijskih sustava : priručnik. Zagreb : Algebra, 2010., str.7

pravodobnu dostupnost podataka. U današnje vrijeme postoje „visoko dostupni sustavi“ (eng. high availability – HA), a njihova arhitektura je usmjerena specifično na postizanje visoke dostupnosti. Nužna karakteristika ovih sustava je da pad ili gubitak jednog elementa ne dovodi do pada sustava, baš naprotiv sustav i dalje funkcionira bez zog elementa.

Dostupnost se može narušiti na nekoliko načina, najčešće je uskraćivanjem usluge u smislu zagušenja primjerice mrežne opreme i poslužitelja, zatim kroz gubitak sposobnosti procesiranja podataka kao razultat prirodnih katastrofa kako što su to poplave, požari i potresi i sl.

Osim navedena tri aspekta u novije vrijeme postoje razmišljanja kako bi u sigurnosni trokut trebalo ubaciti još neke aspekte, a to su dokazivost, autentičnost i neporecivost, no postoje i protivnici ove teze jer smatraju da su ova tri aspekta već uključena u osnovni sigurnosni trokut[20].

Promatrajući trokut informacijske sigurnosti lako se dolazi i do mogućih prijetnji sukladno s aspektima koje trokut čine. Tako se u globalu prijetnje odnose prvenstveno na razotkrivanje u smislu narušavanja tajnosti informacija što je povezano s povjerljivnosti. Kada je riječ o integritetu podataka, njegovo narušavanje može se dogoditi kroz promjene, a prekid rada uzrokuje nedostupnost servisa ili podataka.

Prema svemu sudeći kako bi informacijski sustavi bili djelotvorni i sigurni u svome radu potrebno je da zadovolje sve navedene aspekte.

[20] Sigurnost informacijskih sustava : priručnik. Zagreb : Algebra, 2010., str.7

3. ZAKONSKA REGULATIVA O SIGURNOSTI INFORMACIJSKIH SUSTAVA

Zakona i podzakonskih akta koji reguliraju područje informacijske sigurnosti ima i više nego dovoljno u Republici Hrvatskoj, stoga zbog opširnosti i velike količine zakona poduzeća i organizacije moraju voditi računa da poslovanje provedu u skladu s brojnim zakonima vezanim za ovo područje. U ovom poglavlju biti će riječi o institucijama informacijske sigurnosti u Republici Hrvatskoj, te o samoj zakonskoj reuglativi vezanoj za informacijsku sigurnost. Kroz kratke opise biti će dan uvid u tematiku ovog poglavlja.

3.1. INSTITUCIJE INFORMACIJSKE SIGURNOSTI U REPUBLICI HRVATSKOJ

Uz mnogobrojne zakone koji djeluju na području informacijske sigurnosti također postoji i određeni broj institucija koje brinu za informacijsku sigurnost, a definirati će se područje djelovanja: Nacionalnog CERT-a, CARNet CERT-a, Zavoda za sigurnost informacijskih sustava, Ureda Vijeća za nacionalnu sigurnost, Agencije za podršku informacijskim sustavima i informacijskim tehnologijama, Agencije za zaštitu osobnih podataka te Središnjeg državnog ureda za e-Hrvatsku.

3.1.1. Nacionalni CERT

Nacionalni CERT (eng. Computer Emergency Response Team) osnovan je u skladu sa Zakonom o informacijskoj sigurnosti RH i prema tom zakonu jedna od zadaća je obrada incidenata na Internetu, tj. očuvanje informacijske sigurnosti u RH[21]. Nacionalni CERT preuzet će korake za očuvanje informacijske sigurnosti u obliku uputa, smjernica, preporuka, savjeta i mišljenja samo ukoliko se jedna od strana nalazi na državnim prostorima, odnosno ukoliko u domeni ima „.hr“ ili je IP adresa locirana u državi.

Misija ove institucije je preventivno djelovati te zaštititi sigurnost javnih informacijskih sustava ukoliko se dogodi neki računalni napad, a način na koji to čini je kroz dvije vrste mjera, a to su proaktivne i reaktivne. Proaktivnim mjerama pokušava se spriječiti ili ublažiti moguća šteta, a one uključuju: praćenje stanja na području računalne sigurnosti i objavljivanje sigurnosnih obavijesti u svrhu priprema za sprečavanje šteta, kontinuirano

[21] http://www.cert.hr/onama, 05.06.2014.

praćenje računalno-sigurnosnih tehnologija te se sva nova saznanja prikupljaju i šire, javno objavljivanje novih informacija u svrhu edukacije najšire javnosti i unapređenju svijesti o značaju računalne sigurnosti te provođenje detaljne edukativne obuke za specifične grupe korisnika. Reaktivne mjere služe za suzbijanje incidenata koji ugrožavaju informacijsku sigurnost u RH, pa se njima prikupljaju i distribuiraju sigurnosna upozorenja, pripremaju se i obrađuju sigurnosne preporuke o slabostima u informacijskim sustavima i sve to na javan i ciljan način.

Nacionalni CERT surađuje s relevantnim tijelima RH zaduženim za sigurnost informacijskih sustava kao i sa stranim CERT-ovima preko članstva u Forum of Incident Response and Security Teams (FIRST) i radne grupe TF-CSIRT.

Bitno je naglasiti kako je Nacionalni CERT osnovan 2008. godine u Hrvatskoj, a prije njega je CARNet CERT (C-CERT) koji je djelovao od srpnja 1996. godine, no djelokrug poslovanja C-CERT-a preuzeo je Nacionalni CERT. Osnovna zadaća C-CERT-a bila je koordinacija u procesu rješavanja računalno-sigurnosnih incidenta kod kojih je barem jedna strana uključena u incident morala biti iz Hrvatske. Ciljevi C-CERT-a koji se sada nalaze unutar Nacionalnog CERT-a su poboljšanje ukupne sigurnosti računalnih sustava na mreži, samnjivanje troškova osiguranja računalnih mreža od provala te smanjivanje štete koja je izazvana provalama u računalne sustave.

3.1.2. Zavod za sigurnost informacijskih sustava

Zavod za sigurnost informacijskih sustava (ZSIS) središnje je državno tijelo RH za obavljanje poslova u tehničkim područjima informacijske sigurnosti državnih tijela što obuhvaća standarde sigurnosti informacijskih sustava, sigurnosne akreditacije informacijskih sustava, upravljanje kriptomaterijalima koji se koriste u razmjeni klasificiranih podataka te koordinaciju prevencije i odgovora na računalne ugroze sigurnosti informacijske sigurnosti[22].

ZSIS započinje sa svojim radom 2006. godine i od tada njegov djelokrug poslovanja jest nadziranje tehničkih kriptografskih materijala, upravljanje kriptografskom opremom te koordiniranje Uredom Vijeća za nacionalnu sigurnost. Osim toga, ZSIS-ova uloga je upravljati opremom za kriptografsku zaštitu klasificiranih podataka, zatim provedba

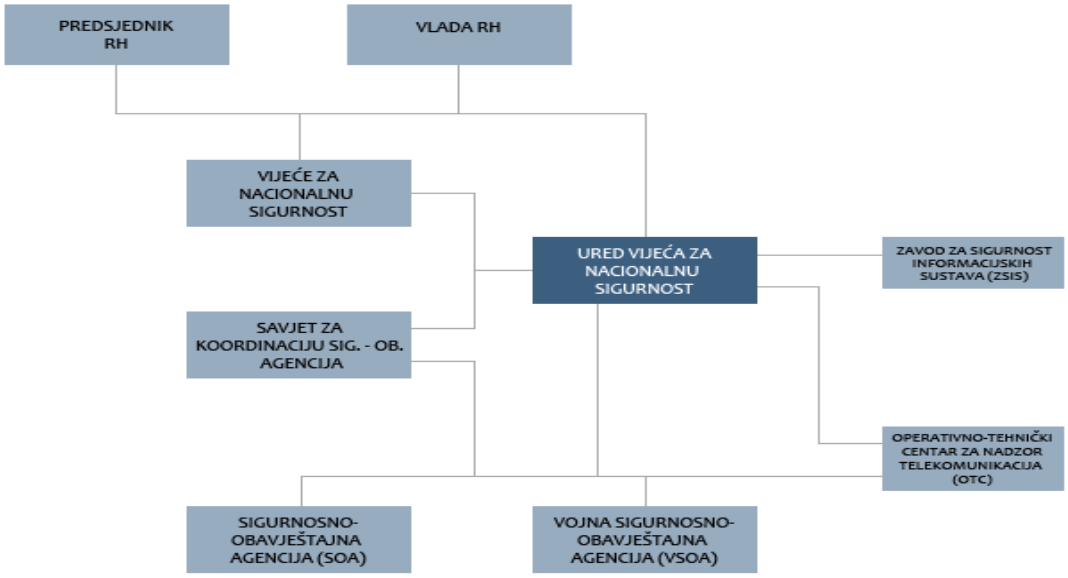
[22] http://hr.wikipedia.org/wiki/Zavod_za_sigurnost_informacijskih_sustava, 05.06.2014.

odgovarajućih procedura te uspostava komunikacijskih kanala za cjelokupnu evidenciju, pohranu, rukovanje te distribuciju kriptografskog materijala. Također, ZSIS provodi sigurnosne akreditacije informacijskih sustava u kojima se koriste klasificirani podaci. Uz već nabrojane mnogobrojne uloge ZSIS-ova zadaća je i trajno uskladiti standarde tehničkih područja sigurnosti informacijskih sustava u RH s međunarodnim standardima i preporukama te osim toga uloga mu je sudjelovanje u nacionalnoj normizaciji na području sigurnosti informacijskih sustava.

3.1.3. Ured vijeća za nacionalnu sigurnost

Ured Vijeća za nacionalnu sigurnost središnje je državno tijelo za informacijsku sigurnost – hrvatski NSA (National Security Authority), koje je zaduženo za donošenje i nadziranje primjene mjera i standarda informacijske sigurnosti[23]. Djelokrug poslovanja ove institucije je područje sigurnosne provjere, fizičke sigurnosti, sigurnosti podataka, sigurnosti informacijskih sustava i sigurnosti poslovne suradnje izdaja certifikata za fizičke i pravne osobe za pristup nacionalnim, NATO i EU klasificiranim podacima. Na slici 4. prikazan je UVNS u sigurnosno-obavještajnom sustavu RH.

Slika 4. UVNS u sigurnosno-obavještajnom sustavu RH.



Izvor: http://www.uvns.hr/default.aspx?id=43, 05.06.2014.

[23] http://www.uvns.hr/default.aspx?id=109, 05.06.2014.

S obzirom da UVNS u Hrvatskoj ima ulogu NSA, skupa sa Vladinom odlukom ima utjecaj u sklapanju međunarodnih sigurnosnih ugovora za zaštitu klasificiranih podataka.

Osnovne zadaće kojima se ova institucija bavi su: izvedba stručnih i administrativnih poslova Vijeća za nacionalnu sigurnost, savjetodavna uloga za koordinaciju sigurnosno-obavještajnih agencija, te poslovi koji Predsjedniku RH i Vlade RH daju nadzor nad radom sigurnosno-obavještajnih agencija i tijela sigurnosno-obavještajnog sustava.

Osim prije navedenih zadaća i uloga UVNS-a, ova institucija donosi određene pravilnike koji zbog uporabe u službene svrhe nisu dostupni javnosti, a oni su:

- Pravilnik o standardima sigurnosne provjere
- Pravilnik o standardima fizičke sigurnosti
- Pravilnik o standardima sigurnosti podataka
- Pravilnik o standardima organizacije i upravljanje područjem sigurnosti informacijskih sustava
- Pravilnik o standardima sigurnosti poslovne suradnje

3.1.4. Agencija za podršku informacijskim sustavima i informacijskim tehnologijama

Agencija za podršku informacijskim sustavima i informacijskim tehnologijama, APIS IT d.o.o.**,** osnovana je krajem 2005. ugovorom između Vlade RH i Grada Zagreba sa svrhom obavljanja poslova razvoja i podrške ključnim informacijskim sustavima RH i Grada Zagreba, te razvijanja aplikativnih servisa i čuvanja potrebnih informacijskih baza[24].

Misija APIS-a je pružiti strateške, stučne i provedbe usluga vlasnicima i javnom sektoru RH u planiranju, razvoju, podršci i održavanju poslovno-informacijskih sustava. Uloga ove institucije u zaštiti informacijske sigurnosti je razvoj i praćenje implementacije smjernica, normi i politike za razvoj e-uprave, razvitak i podupiranje zajedničke računalno-komunikacijske i aplikacijske infrastrukture te podrška tijelima državne uprave u razvoju vlastite strategije e-poslovanja. Sve to postiže na način da štiti osobne podatke, razvija zajedničke elektroničke usluge i centralni pristup informacijskim resursima državne uprave uz odgovarajuću autorizaciju i autentifikaciju te kodiranje i planiranje cjeloživotnog obraovanja državnih službenika u primjeni informacijsko-komunikacijske tehnologije. Cilj

[24] http://hujak.hr/clan-apis-it/, 05.06.2014.

APIS IT-a je biti prvi izbor u pružanju IT servisa u javnom sektoru te postati nacionalni referentni centar razvoja i IT podrške umrežene u korisnički usmjerene uprave RH.

3.1.5. Agencija za zaštitu osobnih podataka

Agencija za zaštitu osobnih podataka osnovana je Zakonom o zaštiti osobnih podataka, a predstavlja samostalno i neovisno tijelo čija je temeljda uloga provedba nadzora nad obradom osobnih podataka u Republici Hrvatskoj.

Vezano uz zaštitu osobnih podataka Agencija obavlja upravne i stručne poslove, a u okviru javnih vlasti to je[25]: nador provođenja zaštite osobnih podataka, ukazivanje na uočene zlouporabe prikupljanja osobnih podataka, sastavljanje liste država i međunarodnih organizacija koje imaju odgovarajuće uređenu zaštitu osobnih podataka , rješavanje povodom zahtjeva za utvrđivanje povrede prava zajamčenih Zakonom o zaštiti osobnih podataka te vođenje Središnjeg registara zbirki osobnih podataka.

Kada je riječ o prikupljanju i korištenju osobnih podataka Agencija za zaštitu osobnih podataka ima pravo brisati prikupljene podatke koji su prikupljeni bez pravne osnove te ukoliko se radi o bilo kakvim nepravilnostima ili radnjama suprotnim zakonu. Osim toga ovlaštenje ove institucije je suradnja s drugim državama i zaštita osobnih podataka ako se osobni podaci iznose van države ili druga neprikladna mjesta.

3.1.6. Središnji državni ured za e-Hrvatsku

Središnji državni ured za e-Hrvatsku središnji je državni ured čiji je zadatak promicanje i sustavno unaprjeđivanje izgradnje informacijsko-komunikacijske infrastrukture u Republici Hrvatskoj, javnog pristupanja internetskim uslugama i sadržajima, razvitka primjene informacijske i komunikacijske tehnologije i sustava elektroničke uprave[26].

U svrhu sigurnosti informacijskih sustava SDUeH igra veliku ulogu jer je u mandatu Vlade Republike Hrvatske između 2011. i 2015. godine organizacijski spojeno Ministarstvo uprave i Središnji državni ured za e-Hrvatsku čime su nadležnosti ministarstva dodani i

[25] http://sigurnost.lss.hr/images/dokumenti/lss-pubdoc-2010-10-003.pdf, 05.06.2014.
[26] http://hr.wikipedia.org/wiki/Sredi%C5%A1nji_dr%C5%BEavni_ured_za_e-Hrvatsku, 05.06.2014.

poslovi informatizacije i modernizacije, a budući da je riječ o spajanju državne uprave i informatizacije ključna je uloga sigurnosti informacijskih sustava.

3.2. ZAKONI IZ PODRUČJA INFORMACIJSKE SIGURNOSTI U RH

S obzirom da je informacijska sigurnost vrlo širok pojam, samim tim logično je da tom oblasti upravlja veliki broj Zakona. U ovom poglavlju biti će navedeni i objašnjeni oni zakoni koji su najbitniji kada je riječ o tematici vezanoj za informacijsku sigurnost, a koje je donio Hrvatski Sabor. Među brojnim zakonima, u ovom objasnit će se: Zakon o informacijskoj sigurnosti, Zakon o zaštiti osobnih podataka, Zakon o tajnosti podataka te Zakon o elektroničkoj ispravi

3.2.1. Zakon o informacijskoj sigurnosti

Zakon o informacijskoj sigurnosti donio je Hrvatski Sabor u srpnju 2007. godine, podijeljen je na 8 cjelina te se putem njega utvrđuju pojmovi informacijske sigurnosti, mjera i standarda informacijske sigurnosti, područja informacijske sigurnosti te nadležna tijela za donošenje, provođenje i nadzor mjera i standarda informacijske sigurnosti[27]. Ovim zakonom utvrđeni su minimalni kriteriji vezani za zaštitu podataka.

Zakon o informacijskoj sigurnosti odnosi se na sva državna tijela, tijela jedinica lokalne i regionalne samouprave te na pravne i fizičke osobe koje u svom poslovanju koriste klasificirane i neklasificirane podatke. Mjere i standardi koje provodi Zakon o informacijskoj sigurnosti prvenstveno se odnose na rad s klasificiranim i neklasificiranim podacima, a utvrđuju se prema stupnju tajnosti, broju, vrsti te mogućnosti ugrožavanja tih podataka na određenoj lokaciji.

Prema članku 8. ovog zakona postoji pet područja za koja se pripisuju mjere i standardi informacijske sigurnosti, a to su:

- Sigurnosna provjera - osobe koje imaju pristup klasificiranim podacima moraju raditi u skladu sa zakonom. Klasifikacija podataka dijeli se u nekoliko stupnjeva, a to je „Povjerljivo“, „Tajno“ i „Vrlo tajno“.

[27] (http://narodne-novine.nn.hr/clanci/sluzbeni/298919.html, 06.06.2014.

- Fizička sigurnost –zaštita mjesta gdje se nalaze klasificirani podaci, odnosno zaštita objekta, prostora i uređaja.
- Sigurnost podataka - opće mjere za prevenciju, otkrivanje i otklanjanje štete od gubitka ili neovlaštenog otkrivanja klasificiranih i neklasificiranih podataka.
- Sigurnost informacijskog sustava – dio informacijske sigurnosti u okviru kojeg se utvrđuju mjere i standardi informacijske sigurnosti klasificiranog i neklasificiranog podatka koji se obrađuje, pohranjuje ili prenosi u informacijskom sustavu te zaštite cjelovitosti i raspoloživost informacijskog sustava u procesu planiranja, projektiranja, izgradnje, uporabe, održavanja i prestanka rada informacijskog sustava.
- Sigurnost poslovne suradnje – provedba natječaja ili ugovora s klasificiranom dokumentacijom koji obvezju pravne i fizičke osobe.

Zakonom o informacijskoj sigurnosti određena su središnja državna tijela koja imaju ulogu u informacijskoj sigurnosti, a koja su detaljnije opisana u točki 3.1. ovog rada, pa će sada biti samo navedena: Ured Vijeća za nacionalnu sigurnost, Zavod za sigurnost informacijskih sustava te Nacionalni CERT.

Nadzor informacijske sigurnosti provode savjetnici za informacijsu sigurnost, a njihovi poslovi su nadzor organizacije, provedbe te učinkovitosti propisanih mjera i standarda informacijske sigurnosti u tijelima i pravnim osobama.

3.2.2. Zakon o zaštiti osobnih podataka

Zakon o zaštiti osobnih podataka donio je Hrvatski Sabor u lipnju 2003. godine, te se ovim Zakonom uređuje zaštita osobnih podataka o fizičkim osobama te nadzor nad prikupljanjem, obradom i korištenjem osobnih podataka u Republici Hrvatskoj[28]. Zakon o zaštiti osobnih podataka podijeljen je na 11 cjelina: temeljne odredbe, obrada osobnih podataka, obrada posebnih kategorija osobnih podataka, povjeravanje poslova obrade osobnih podataka, davanje podataka korisnicima, iznošenje osobnih podataka iz Republike Hrvatske, zbirke osobnih podataka, evidencije i središnji registar, prava ispitanika i zaštita prava, nadzor nad obradom osobnih podataka, kaznene odredbe te prijelazne i zaključne odredbe.

[28] http://narodne-novine.nn.hr/clanci/sluzbeni/305952.html, 06.06.2014.

Svrha zakona o zaštiti osobnih podataka je zaštita privatnog živora, odnosno zaštita ostalih ljudskih prava i temeljnih sloboda u prikupljanju, obradi i korištenju osobnih podataka. Ta prava osiguravaju se svakoj fizičkoj osobi bez obzira na: državljanstvo i prebivalište, tj. neovisno o rasi, boji kože, spolu, jeziku, vjeri, zatim o političkom ili drugom uvjerenju, o nacionalnom ili socijalnom podrijetlu te neovisno o imovini, rođenju, naobrazbi, društvenom položaju ili drugim osobinama. Unutar ovog zakona djeluje Agencija za zaštitu osobnih podataka (AZOP) i njena uloga je nadzor za obradu osobnih podataka, te joj je propisan ustroj, financiranje, rukovodstvo, ovlasti i dužnosti te poslovi i funkcije koje smije obavljati.

Zakonom je definiran pojam osobnog podatka, obrada osobnih podataka, zbirka osobnih podataka, voditelj zbirke osobnih podataka, korisnik, privola ispitanika, osnovni oblik evidencije informacija o zbirci podataka koju voditelj zbirke mora voditi. Svaka evidencija se mora dostaviti Agenciji za zaštitu podataka, te joj se mora prijaviti svaka izmjena i obrada. Osim toga definirano je koja prava imaju ispitanici s obzirom na dane podatke, kako postupati s neispravnim ili nepotpunim padacima, zatim mogućnost podnošenja Agenciji za zaštitu osobnih podataka zahtjeva za utvrđivanje povrede prava koji su zajamčeni ovim zakonom, utvrđivanje radnji koje se mogu poduzimati na temelju rješenja predhodno spomenutog zahtjeva, princip poslovnih podataka kojeg se moraju pridržavati svi zaposlenici AZOP-a, te kazne u raznim slučajevima kršenja odredbi ovog zakona koje se kreću između 20.000 i 40.000 kuna.

Zakonom o zaštiti osobnih podataka propisani su uvjeti pod kojima se mogu prikupljati i obrađivati podaci. U skladu s time određeno je koje je podatke zabranjeno prikupljati i u kojim iznimnim slučajevima se ti podaci mogu ipak prikupiti, navedeni su uvjeti koje voditelj zbirke (ili osobnih podataka ili izvršitelj obrade) moraju ispuniti prema ispitaniku kako bi mogli izvršavati prikupljanje i obradu njegovih osobnih podataka. Zakonom su propisane i mogućnosti imenovanja izvršitelja obrade od strane voditelja zbirke i njegove obveze, zatim kada voditelj smije, a kada ne smije dati osobne podatke na korištenje, koji je vremenski interval u kojem se mogu koristit određeni podaci te su definirani uvjeti iznošenja osobnih podataka van države.

3.2.3. Zakon o sigurnosno – obavještajnom sustavu RH

Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske je donio Hrvatski sabor u srpnju 2006. godine i sastoji se od 10 cjelina koje su u njemu obrađene i to ovim redoslijedom[29]: temeljne odredbe, Vijeće za nacionalnu sigurnost, Savjet za koordinaciju sigurnosno-obavještajnih agencija, Ured Vijeća za nacionalnu sigurnost, Zavod za sigurnost informacijskih sustava, Operativno-tehnički centar za nadzor telekomunikacija, zatim sigurnosno-obavještajne agencije, poslovi i ovlasti sigurnosno-obavještajnih agencija, suradnja sigurnosno – obavještajnih agencija, ustrojstvo i upravljanje sigurnosno – obavještajnim agencijama, položaj, prava, obveze i odgovornosti te način utvrđivanja plaća dužnosnika i zaposlenika sigurnosno – obavještajnih agencija, ureda vijeća za nacionalnu sigurnost, zavoda za sigurnost informacijskih sustava i operativno – tehničkog centra za nadzor telekomunikacija, nakon toga nadzor nad sigurnosno – obavještajnim agencijama, sredstva za rad sigurnosno – obavještajnih agencija, Ureda Vijeća za nacionalnu sigurnost, Zavoda za sigurnost informacijskih sustava i Operativno – tehničkog centra za nadzor telekomunikacija te prijelazne i završne odredbe.

Ovaj zakon ima dvije najvažnije odrednice, a to su:

- Sigurnosno-obavještajna agencija (SOA) – Prikuplja podatke korištenjem javnih izvora, komunikacijom s građanima ili potraživanjem službenih podataka od državnih tijela, tijela jedinica lokalne i regionalne samouprave. Ima pravo tajnog prikupljana podataka od građana, a uloga joj je sprječavanje bilo kakvih radnji koje bi mogle ugroziti sigurnost državnih tijela, građana i nacionalnih interesa putem terorističkih djelovanja ili nekog drugog oblika nasilja, neovlaštenog ulaska u zaštićene informacije i komunikacijske sustave državnih tijela te bilo kojih drugih aktivnosti koje su usmjerene na ugrožavanje nacionalne sigurnosti.
- vojna sigurnosno-obavještajna agencija (VSOA) – Uloga joj je izvršavanje zadaća obrane suvereniteta, neovisnosti te teritorijalne cjelovitosti RH. Ova agencija može primjenjivati mjere tajnog prikupljanja podataka (tajni nadzor telekomunikacijskih usluga, sadržaja komunikacija, tajni nadzor lokacije korisnika, tehničko snimanje unutrašnjosti objekta, zatvorenih prostora, tajno praćenje i motrenje uz zvučno snimanje) kojima se privremeno ograničavaju neka ustavna ljudska prava i slobode

[29] http://www.propisi.hr/print.php?id=5045, 06.06.2014.

prema pripadnicima Ministarstva obrane i Oružanih snaga, ali to čini samo u slučajevima kada na drugi način ne može doći do podataka.

Poslovi i ovlasti sigurnosno-obavještajnih agencija su prikupljanje podataka, evidencija podataka i njihovo korištenje, zatim sigurnosne provjere i protuobavještajna zaštita, mjere prikrivanja, izvještavanje te strategijsko elektoničko izviđanje za potrebe sigurnosno – obavještajnih agencija. Sam nadzor nad sigurnosno –obavještajnim agencijama vrši Hrvatski Sabor, odnosno Ured Vijeća za nacionalnu sigurnost, te Vijeće za grđanski nadzor sigurnosno- obavještajnih agencija.

Unutar ovog zakona djelokrug je raznih tijela, pa tako Vijeće za nacionalnu sigurnost razmatra i procjenjuje obavještajne i sigurnosne prijetnje te rizike, Savjet za koordinaciju sigurnosno – obavještajnih agencija provodi odluke predsjednika RH i Vlade oko usmjeravanja rada SOA, Ured Vijeća za nacionalnu sigurnost obavlja stručne i administrativne poslove za Vijeće nacionalne sigurnosti i Savjet za koordinaciju sigurnosno-obavještajnih agencija, Zavod za sigurnost informacijskih sustava je središnje državno tijelo za obavljanjee poslova u tehničkom području informacijske sigurnosti RH, te Operativno-tehnički centar za nadzor telekomunikacija obavlja aktivacije i upravljanje mjerom tajnog nadzora telekomunikacijskih usluga.

3.2.4. Zakon o elektroničkoj ispravi

Zakon o elektroničkoj ispravi stupa na snagu 29. prosinca 2005. godine. Ovim Zakonom se uređuje pravo fizičkih i pravnih osoba na uporabu elektroničke isprave u svim poslovnim radnjama i djelatnostima te u postupcima koji se vode pred tijelima javne vlasti u kojima se elektronička oprema i programi mogu primjenjivati u izradi, prijenosu, pohrani i čuvanju informacija u elektroničkom obliku, pravna valjanost elektroničke isprave te uporaba i promet elektroničkih isprava[30].

Svaka osoba odlučuje da li će prihvatiti ili neće prihvatiti uporabu i promet elektroničkih isprava za svoje potrebe i potrebe poslovnih i ostalih odnosa s drugima. Neovisno da li je određena osoba prihvaća ili ne, elektronička isprava ima istu pravnu snagu kao i isprava na papiru ako se njena uporaba provodi u skladu s odredbama ovog Zakona.

[30] http://www.zakon.hr/z/272/Zakon-o-elektroni%C4%8Dkoj-ispravi, 09.07.2014.

Prema ovom zakonu elektronička isprava definirana je kao jednoznačno povezan cjelovit skup podataka koji su elektronički oblikovani (izrađeni pomoću računala i drugih elektroničkih uređaja), poslani, primljeni ili sačuvani na elektroničkom, magnetnom, optičkom ili drugom mediju, i koji sadrži svojstva kojima se utvrđuje izvor (stvaratelj), utvrđuje vjerodostojnost sadržaja te dokazuje postojanost sadržaja u vremenu. Sadržaj elektroničke isprave uključuje sve oblike pisanog teksta, podatke, slike i crteže, karte, zvuk, glazbu, govor[31].

Kada je riječ o radnjama uklljučenim u dokumentacijski ciklus, elektronička isprava morala bi osigurati jednoznačno obilježje kojim se nedvojbeno utvrđuje pojedinačna elektronička isprava te pojedinačni stvaratelj elektroničke isprave, zatim informacijsku cjelovitost i nepovredivost elektroničke isprave, oblik zapisa koji čitatelju omogućuje jednostavno čitanje sadržaja te pristup sadržaju elektroničke isprave kroz cijelo vrijeme dokumentacijskog ciklusa.

Elektronička isprava sastoji se od dva neodvojiva dijela, općeg i posebnog. Opći dio čini predmetni sadržaj isprave, odnosno informacije elektroničkom obliku. Posebni dio sastavljen je od jednog ili više integriranih elektroničkih potpisa i podataka o vremenu nastajanja elektroničke isprave te drugih dokumentacijskih svojstva[32].

Uporaba elektroničke isprave ni jednoj strani ne smije ograničavati poslovanje ili ju dovoditi u neravnopravan položaj. Za uprabu elektroničkih isprava može se koristiti bilo koja upotrebljiva i dostupna informacijsko-komunikacijska tehnologija, ukoliko nije Zakonom drugačije određeno. Cjelokupni informacijski sustav koji se koristi u radnjama s elektroničkim ispravama mora imati odgovarajuću zaštitu osobnih podataka te je bitno da postoji mogućnost provjere vjerodostojnosti, izvornosti te nepromjenjivosti elektroničke isprave.

Kada su ispunjenji sljedeći uvjeti, uporaba elektroničkih isprava je pravovaljana:

- da elektronička isprava sadrži podatke o stvaratelju, pošiljatelju i primatelju te podatke o vremenu otpreme i prijema,

[31] http://www.poslovniforum.com/nnhr/2005-12-150-2898.html, 30.07.2014.

[32] http://www.zakon.hr/z/272/Zakon-o-elektroni%C4%8Dkoj-ispravi, 30.07.2014.

- da elektronička isprava kroz cijeli dokumentacijski ciklus sadrži isti unutarnji i vanjski obrazac koji je oblikovan pri njenoj izradi i koji mora ostati nepromijenjen kroz bilo koje radnje u postupcima njene otpreme i uporabe,
- da je elektronička isprava u bilo kojem trenutku dostupna i čitljiva ovlaštenim fizičkim i pravnim osobama.

Kada je riječ o zaštiti elektroničkih isprava postoji nekoliko postupaka koje treba poštivati. Pri korištenju elektroničkih isprava potrebno je primjenjivati odgovarajuće tehnološke postupke i opremu kojom se omogućuje zaštita postupaka i elektroničkih isprava. Informacijski posrednik javlja se s ulogom osiguranja zaštite postupaka i elektroničkih isprava kada se koristi informacijska oprema i komunikacijski sustav informacijskog posrednika. Oprema za zaštitu elektroničkih isprava s tajnim podacima koje koriste tijele javne vlasti, obavezno se ovjerava od strane nadležnog rijela zaduženog za poslove informacijske sigurnosti.

Kada je riječ o kaznama za nepoštivanje pravila i propisa za prometovanje elektroničkim ispravama one se kreću od minimalno 5.000 kuna do čak 60.000 kuna za pravne osobe, a za fizičke od 500 do 3.000 kuna.

Osim navedenih i objašnjenih zakona koji su od velike važnosti za sigurnost informacijskih sustava u RH postoji i duži niz ostalih Zakona koji se tiču ove oblasti. S obzirom da su predhodnih nekoliko zakona detaljno objašnjeni, biti će navedena samo imena nekih od ostalih Zakona vezanih za sigurnost informacijskih sustava. Pa je tako bitno naglasiti ove zakone: Zakon o elektroničkom potpisu, Zakon o Privatnoj zaštiti, Zakon o arhivu i arhivskoj građi, Zakon o telekomunikacijama, Zakon o računovodstvu, Zakon o zaštiti tajnosti podataka i slično.

3.3. NORME INFORMACIJSKE SIGURNOSTI

S obzirom na činjenicu da je sigurnost informacijskih sustava u današnjici postigla vrlo visoku razinu za potrebe regulacije i implementacije sigurnosti u organizacijama određene su norme tj. standardi. Prema njima se osigurava pravilno funcioniranje sigurnosnih sustava u određenoj organizaciji. Standardi koji su od velike važnosti za sigurnost informacijskih sustava su: ISO 27001:2005 – Sustav upravljanja informatičkom sigurnošću, te ISO 27002:2013– Kodeks postupaka za upravljanje informacijskom

sigurnošću. Kako bi se uspostavio kvalitetan sustav za upravljanje sigurnošću informacija potrebno je koristiti oba dva standarda.

ISO 27002 i ISO 27001 su glavni međunarodni standardi informacijske sigurnosti, koji su objavljeni od strane Internacionalne organizacije za standardizaciju (ISO). ISO 27002 preimenovan je 2007. godine, a ranije je bio poznat kao ISO 17799. Najnovija verzija ISO 27002 norme je ona iz 2013. godine. ISO 27002 usko je povezan sa ISO 27001 standardom[33].

Veliku važnost ovim standardima pridaje činjanica da ih je moguće primjeniti na gotovo sve organizacije jer osiguravaju fleksibilnost, definiraju upravljački okvir, a ne ulaze u konkretnu tehničku implementaciju.

Osim već naglašenih standarda, postoje i mnogi drugi vezani uz problematiku zaštite i sigurnosti informacijskih sustava, koji su već doneseni ili su planirani u narednom razdoblju[34]:

- ISO 27000 – Rječnik termina koji se koriste unutar ISO 27000 serije standarda
- ISO 27001:2005 – Sustav upravljanja informatičkom sigurnošću (ISMS)
- ISO 27002:2013– Kodeks postupaka za upravljanje informacijskom sigurnošću
- ISO 27003 – Vodič za implementaciju ISMS-a
- ISO 27004 – Mjerenje i metrika efikasnosti sustava informacijske sigurnosti
- ISO 27005 – Upravljanje rizicima informacijske sigurnosti
- ISO 27006:2007 – Zahtjevi za postupkom analize i certificiranja standarda
- ISO 27007 – Upute za analizu ISMS-a
- ISO 27011 – Upute za uspostavu ISMS u telekomunikacijskom sektoru
- ISO 27031 – Specifikacije za ICT odjel pripremljenosti poslovne neprekinutosti rada
- ISO 27032 – Upute za cyber- sigurnost
- ISO 27033 – Upute za mrežnu sigurnost
- ISO 27034 – Upute za sigurnost aplikacija
- ISO 27799 – Sigurnosni sustav u zdravstvu

[33] http://iso-17799.safemode.org/, 30.07.2014.
[34] http://os2.zemris.fer.hr/ISMS/2008_poljak/Poljak_Ivan_diplomski_rad_1716.pdf, 30.07.2014.

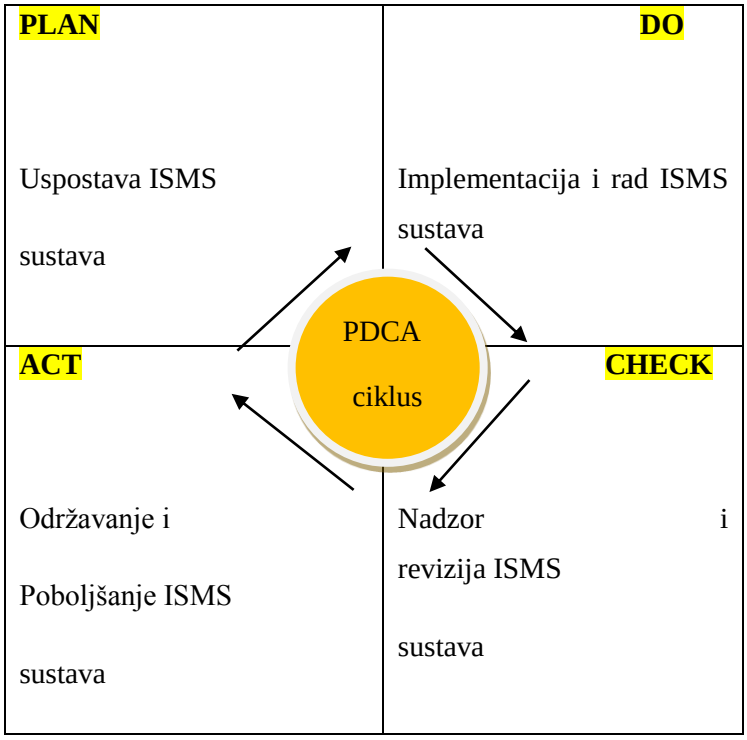
Sada kada je dan prikaz cijele serije standarda ISO 27000, u nastavku će detaljnije biti opisane skupine standarda ISO 27001 i ISO 27002, koje se smatraju najvažnijim kada je riječ o sigurnosti informacijskih sustava.

3.3.1. ISO 27001 – Sustav upravljanja informatičkom sigurnošću

ISO 27001:2005 temeljni je standard ISO 27000 serije standarda, a definira zahtjeve za uspostavu, implementaciju, rad, nadzor, reviziju, održavanje i poboljšavanje dukumentiranog sustava upravljanja informacijskom sigurnošću[35]. Ova norma jednostavnim riječima objašnjeno služi za postavljanje temelja informacijske sigurnosti i određivanje njezinih okvira.

Kako bi uspješno provela svoje zadatke ova norma koristi procesni pristup koji omogućuje razumijevanje sigurnosnih zahtjeva organizcacije i potrebu za uspostavom ciljeva na području informacijske sigurnosti. Na slici 5. prikazan je PDCA model kojeg usvaja norma ISO 27001 za uspješno provođenje svojih zadataka.

Slika 5. PDCA model



Izvor: izradila studentica

[35] Sigurnost informacijskih sustava : priručnik. Zagreb : Algebra, 2010., str. 60

PDCA ciklus, odnosno model sastoji se od četiri koraka: Plan, Do, Act i Check. Plan odnosno planiranje označava uspostavu ISMS politike, ciljeva, procesa i procedura za upravljanje rizikom i poboljšanje informacijske sigurnosti. Do tj. primjena odnosi se na implementaciju i rad ISMS kontrola, procesa i procedura. Check – provjera jest procjena i mjerenje učinkovitosti procesa, kontrola i ciljeva te priprema izvještaja za reviziju ISMS sustava. Posljednji korak u ovom modelu je Act – djelovanje, a označava poduzimanje korektivnih i preventivnih mjera na temelju rezultata interne revizije i revizije uprave i ostalih relevantnih informacija u cilju poboljšanja ISMS sustava[36].

Sukladno PDCA modelu koji je primjenjen u oblikovanju ISMS-a, postoje četiri faze sustava upravljanja informacijskom sigurnošću koje definira norma ISO 27001. Prema tome faza planiranja služi da se isplanira osnovna organizacija informacijske sigurnosti, postave ciljevi za informacijsku sigurnost i da se odaberu primjerene sigurnosne mjere. U fazi implementacije provodi se sve što se isplaniralo tijekom prethodne faze. Svrha faze praćenja i pregledavanja jest da se kroz razne „kanale" nadgleda kako funkcionira ISMS, i da li rezultati ispunjavaju postavljene ciljeve, dok faza održavanja i poboljšavanja je da se poboljša sve što je u prethodnoj fazi identificirano kao nesukladno[37]. Važno je naglasiti kako se ciklus nikad ne prekida, odnosno ove četiri faze moraju se odvijati ciklički kako bi ISMS pravilno funkcionirao.

Postoji određena dokumentacija koju koristi ISO 27001, a količina te dokumentaciji ovisi o veličini organizacije na koju se norma primjenjuje. Dokumentacija koju zahtjeva ISO 27001 jest[38]:

- opseg ISMS-a
- politika ISMS-a
- procedure za upravljanje dokumentacijom, za interne audite, te za korektivne i preventivne mjere
- sve ostale dokumente ovisno o odabranim sigurnosnim mjerama
- metodologiju za procjenu rizika
- izvješće o procjeni rizika
- izvješće o primjenjivosti

[36] Sigurnost informacijskih sustava : priručnik. Zagreb : Algebra, 2010., str. 63
[37] http://www.iso27001standard.com/hr/sto-je-iso-27001, 30.07.2014.
[38] http://www.iso27001standard.com/hr/sto-je-iso-27001#dokumentacija, 30.07.2014.

- plan obrade rizika
- zapise

Kao što je već navedeno o veličini organizacije ovisi količina potrebne dokumentacije stoga je logično da će manje organizacije zahtjevati svega destak dokumenata, dok će veće organizacije tražiti čak i do nekoliko stotina dokumenata u svom ISMS-u.

Međunarodno priznat ISO 27001 certifikat dobivaju one organizacije koje ostvare certifikaciju sustava upravljanja informacijskom sigurnošću, stoga se upravo ovaj standard (ISO 27001) smatra temeljem za certifikaciju sustava upravljanja informacijskom sigurnošću. Iako je ISO 27001:2005 još uvijek važeći, na tržištu se pojavila poboljšana verzija iste norme ISO 27001:2013, koja će se od 1.listopada 2015. godine primjenjivati na sve organizacije.

3.3.2. ISO 27002 - Kodeks postupaka za upravljanje sustava informacijske sigurnosti

ISO 27002 je norma koja detaljnije opisuje na koji način provesti pojedine mjere zaštite iz ISO 27001. Ova norma prvenstveno je nosila naziv ISO/IEC 17799, a preuzeta je iz prvog dijela BS 7799 standarda "Code of Practice for Information Security Management". Ime ove norme mijenja se u srpnju 2007. godine kada postaje ISO/IEC 27002 te predstavlja međunarodnu osnovu za razumijevanje i upravljanje informacijskom sigurnošću, a sastoji se od 11 domena koje opisuju sigurnosne kontrole. Tih 11 domena sastoji se od 39 kontrolnih ciljeva te 133 kontrola koje se koriste u identifikaciji, upravljanju i smanjenju cijelog niza prijetnji kojima se informacije svakodnevno izlažu[39].

Kako bi se kontrole i kontrolni mehanizmi implementirali u skladu s uputama unutar ISO 27001, potrebne su smjernice koje nudi norma ISO 27002. ISO 27002 je norma koja detaljnije opisuje zadatke norme ISO 27001 te je bitno naglasiti kako ona nije upravljačka norma stoga se po njoj ne može certificirati.

Sigurnosne mjere u normi ISO 27002 nose iste nazive kao i one u Aneksu A norme ISO 27001 pa tako u normi ISO 27002 mjera 6.1.5 ima naslov Sporazumi o tajnosti, te u normi ISO 27001 pod istim imenom A.6.1.5 Sporazumi o tajnosti. Razlika između ove dvije

[39] Bogati, J., NORME INFORMACIJSKE SIGURNOSTI ISO/IEC 27K ,Praktični menadžment, Vol. II, br. 3, str. 112-117, **str 113, 2011 godina, file:///C:/My%20Documents/Downloads/PM_br3_cl17%20(1).pdf,**

norme, zapravo je u količini detalja koji su posvećeni određenoj sigurnosnoj mjeri. Tako je za isti naslov odnosno sigurnosnu mjeru u normi ISO 27001 izdvojena tek jedna rečenica, dok je u normi ISO 27002 detaljno opisana ta ista sigurnosna mjera na način da je za nju izdvojeda gotovo cijela stranica[40].

Prošle 2013. godine izašla je nova inačica ove norme, koja se krajem 2013. godine i počela primjenjivati iako su u funkciji još uvijek stara ISO 27001:2005 te ISO27002:2007. Na Tablici 2. prikazana je razlika po domenama od čega se sastojala prošla verzija ovog standarda i od čega se sastoji nova verzija.

Tablica 2. Sadržaj ISO 27002:2005 i ISO 27002:2013

ISO 27002:2005	**ISO 27002:2013**
Security Policy	Information Security Policies
Organization of Information Security	Organization of Information Security
Asset Management	Human Resources Security
Human Resources Security	Asset Management
Physical and Environmental	Access control
Communications and Operations Management	Cryptography
Access Control	Physical and environmental Security
Information Systems Acquisition	Operations Security
Information Security Incident Management	Communications Security
Business Continuity Management	System Acquisition, Development and Maintenance
Compliance	Supplier Relationships
	Information Security Incident Management
	Information Security Aspects of Business Continuity Management
	Compliance

Izvor: izradila studentica

[40] http://security.foi.hr/wiki/index.php/ISO_27002_-_Norma_i_Sukladnost, 02.08.2014.

Za razliku od verzije koja je zaživila 2007.godine u novoj verziji ove norme ima nekoliko izmjena. Najbitnija izmjena u verziji ISO 27002:2013 je potpuno uklanjanje poglavlja o procjeni i obradi rizika. Također su i mnoga druga područja kontrola izbrisana upravo zbog toga što su te kontrole sadržane već u nekim drugim odjeljcima ili standardima[41]. Nova verzija umjesto 133 kontrole sada sadrži samo 114, a broj domena se sa 11 povećao na 14.

Kao što se vidi iz tablice, najveće promjene, odnosno dodatna područja su vezana uz kriptografiju, komunikacijsku sigurnost te odnose između dobavljača. Bez obzira na to što je broj domena porastao cjelokupna struktura odnosno količina stranica ove norme se smanjila, jer se više fokusira na određeni problem, kontrolu i dio koji zahvaća. Iako su nazivi domena različiti, pregrupirani su u novoj normi kako bi bili što praktičniji za djelovanje. Također jedna od promjena u novoj normi jest terminologija. Pa je tako primjerice riječ „password“ zamjenjena sa „secret authentication information“, zatim„check“ sa „verify i slično. Iz svega navedenog može se zaključiti da promjene u strukturi kontrola rješavaju niz nedorečenosti, dupliranja i nelogičnosti.

[41] http://blog.iso27001standard.com/2013/02/11/main-changes-in-the-new-iso-27002-2013-draft-version/, 31.07.2014

4. MJERE ZAŠTITE INFORMACIJSKIH SUSTAVA

Sigurnost informacijskih sustava i sama zaštita podataka i informacija dobiva na važnosti tek kada su se počela primjenjivati računala u poslovnoj praksi. Tada se veća pažnja usmjerila na zaštitu informacijskih sustava te su uvedeni razni standardi vezani uz rad računala i pohranjivanje te zaštitu podataka i informacija. Na samom začetku informatizacije, računalna oprema bila je centralizirana pa je iz tog razloga najznačajniji način zaštite bila upravo fizička zaštita. Fizička zaštita primjenjivala se iz razloga što se računalna oprema nalazila u posebnim prostorijama i objektima, a te prostorije i objekte trebalo je dobro čuvati kako bi se informacije zaštitile. Trenutak kada se širi potreba i za nekim drugim vrstama zaštite je kada se počela distibuirati oprema te kada su se podaci uključivali na internet. Tada je bilo potrebno osim fizičke zaštite uvesti i druge vrste zaštite kao što su hardversko softverska zaštita te organizacijsko administrativna zaštita, te cjelokupan sustav zaštite svesti na složeniju razinu. Uvođenjem novih vrsta zaštite informacijskih sustava naglašena je potreba izradom i primjenom raznih uputa o zaštiti podataka koje se primjenjuju u poduzećima.

Informacijska sigurnost je zaštita informacija od velikog broja prijetnji radi osiguranja kontinuiteta poslovanja, smanjenja poslovnog rizika i povećanja prihoda od investicija i poslovnih prilika. Informacijska sigurnost postiže se primjenom odgovarajućeg skupa kontrola, uključujući politike, procese, procedure, organizacijske strukture i softverske i hardverske funkcije[42].

Prema navedenom mjere zaštite informacijskih sustava mogu se podijeliti na zaštitu na razini države, zaštitu samih podataka, programsku zaštitu, organizacijsku zaštitu, te fizičku i tehničku zaštitu. Budući da su neki načini prethodno opisani u radu poput zaštite samih podataka i informacija do zaštite na razini države te su navedeni i objašnjeni zakonski akti koji se koriste na području informacijske sigurnosti, u daljenjem radu biti će navedeni te opisani preostali načini kojima se vrši zaštita informacijskih sustava.

[42] Hadjina, N. Zaštita informacijskih susava. Zagreb: FER, 2009., str 6

4.1. HARDVERSKO SOFTVERSKA ZAŠTITA

Kada je riječ o hardversko softverskoj zaštiti informacijskih sustava bitno je naglasiti kako je upravo ovaj aspekt jedan od najranjivijih. Razlog tome je što u današnjici jednostavnu i brzu distribuciju softvera omogućuju sve brže internet veze te činjenica da upravo računalna mreža postaje glavni medij kojim se sve to omogućuje. Budući da je razvoj softvera relativno skup potrebno ga je štititi iako to nije moguće u potpunosti. Kad tada će se pojaviti piratska verzija na internetu te neće biti potrebe za originalnim programom. Ne postoji određena metoda kojom je moguće u potpunosti zaštiti softver te se iz tog razloga upravo i pojavljuju piratske verzije nakon nekog vremena što je program izbačen na tržište. Svaki program, odnosno softver predstavlja vid zaštite podataka i korištenjem razvijenog softvera i pravilnim očuvanjem istog poduzeće postiže prednost nad konkurencijom i veću zaradu.

4.1.1. Zakonska zaštita softvera

Postoje razni načini kojima se zakonski softver može zaštititi. Razlog tome je što se softver može smatrati i kao vrstom literarnog djela te kao vrstomm mehanizma koji obavlja neki koristan posao. Upravo zbog toga softver se može štititi kroz autorsko pravo, patent, te licencu.

Autor se od nelegalnog korištenja njegova djela koristi autorskim pravom, ali ne štiti se sama ideja već način prikaza neke ideje te originalna implementacija. U softverskoj industriji autorskim pravom moguće je zaštititi izvorni i izvršni kod programa, strukturu i organizaciju koda programa, dijelove ili cijelo korisničko sučelje te sve priručnike, upute i ostalu dokumentaciju u pisanom ili digitalnom obliku[43]. Softver se štiti autorskim pravom jer se vrlo jednostavno, jeftino i u kratkom roku može dobiti, a također je primjenjivo na gotovo svaki oblik softvera.

Za razliku od autorskog prava, patentom se štiti sama ideja, matematički postupci korišteni u programu te algoritmi. U softverskoj industriji patent se konkretno odnosi na svaki koristan proizvodni proces, mehanizam ili princip koji je nov, te se ne nalazi prethodno u nekom već objavljenom patentu. Što se tiče patentiranja softvera ono se smatra najmoćnijim načinom zaštite softvera ali u isto vrijeme nije ni najpametnije činiti zaštitu

[43] http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2004-04-71.pdf, 16.08.2014.

putem patentiranja[44]. Činjenica je da je za patentiranje potrebno i do nekoliko godina, pa to dovodi u pitanje da li se isplati patentirati neki softver koji će za par godina biti neiskoristiv. Softver se u današnje vrijeme prebrzo razvija da bi ga se ograničilo patentiranjem. U SAD-u je moguće patentirati softver ali u Europi nije.

Licencom se određuje koliko dugo se smije koristiti neki softver, u koje svrhe se koristi te koliko računala smije taj isti softver instalirati. Softverska licenca je pravni instrument kojim se regulira korištenje, distribucija i redistribucija softvera[45]. U današnje vrijeme najčešća zaštita softvera je upravo putem neke vrste licence.

Zakonski oblik zaštite dijeli softver na nekoliko kategorija. Te kategorije su: Public domain, Open Source, Freeware, Shareware, Komercijalni softver te licencirani Komercijalni softver[46]. Razlika svakog od ovih kategorija je u razini radnji i dozvola koje krajnji korisnik ima pravo činiti s određenim softverom. Stoga je Public domain softver s kojim korisnik radi sve što želi, smije ga koristiti, umnožavati, distribuirati pa čak i prodavati, a da prethodno nije dobio odobrenje autora. Redom kako su navedene kategorije softvera sve je manje ovlasti koje krajnji korisnik ima što se tiče njegovog korištenja, distribucije, kopiranja i sl. Ono što omogućuje Open Source softver jest promjena izvornog koda i daljnja distribucija istog pod uvjetom da i takav izmjenjeni softver ostaje Open Source, a sve se distribuira pod istim licenčnim sporazumom. Freeware je softver koji ne odobrava promjene, te ima posebnu licencu sa definiranim pravilima korištenja, a autor softvera zadržava autorsko pravo. Shareware softver najsličniji je Freeware-u, samo što se nakon određenog perioda za njegovo korištenje treba izdvojiti određena svota novca kako bi se takav softver nastavio koristiti. Komercijalni softver je kategorija softvera gdje korisnik ima pravo samo koristiti taj softver, a nesmije ga kopirati, mijenjati te distribuirati. Danas je najčešće korištena kategorija licenciranog komercijalnog softvera. Kako sam naziv kaže, ovim softverom dobiva se samo licenca za korištenje istog, te ga je moguće koristiti u skladu s licenčnim sporazumom te zakonom o autorskim pravima.

4.1.2. Metode zaštite softvera

U pokušaju da se softver zaštiti koriste se razne hardverske i softverske metode. Pomoću tih metoda prije nego se omogući korištenje softvera potrebno je proći kroz neku

[44] http://www.itvestak.org.rs/ziteh_04/radovi/ziteh-28.pdf,
[45] http://www.digitconsulting.rs/index.php/licenciranje-microsoft/licenciranje/sofverska-licenca.html, 16.08.2014.
[46] http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2004-04-71.pdf, 16.08.2014.

vrstu autentikacije korisnika, kako bi osigurale zaštitu informacija. U daljnjem tekstu u kratkim crtama biti će riječi o uređaju Dongle, zaštiti pomoću instalacijskog medija, zaštiti CD-a protiv kopiranja, fiksnoj registracijskoj šifri, promjenjivoj registracijskoj šifri, serijskom broju ovisnom o hardveru te zaštiti programa pomoću registracijske datoteke.

Dongle je vrsta hardvera koji se koristi kako bi se zaštitio neki softver od kopiranja i nedopuštenog korištenja[47]. To je zapravo uređaj koji se spaja na serijski ili paralelni komunikacijski port računala da bi se omogućilo pokretanje određene aplikacije, drugim riječima takav uređaj sadrži hardverski implementiran ključ pomoću kojega se pristupa određenoj aplikaciji. Preko određenih portova računala prema dongle-u aplikacija šalje upite i provjerava odgovore koji pristižu. Ukoliko odgovarajući dongle nije priključen aplikacija će prestati s radom jer neće dobiti potrebne odgovore u obliku šifri. Što se tiče same razine zaštite ona nije određena dongle uređajem već izvedbom aplikacije koju koristi. Razloza zašto se u današnjici dongle uređaji ne koriste ima nekoliko, počevši od kompliciranе instalacije, visoke cijene pa sve do nemogućnosti distribucije softvera preko Interneta.

Zaštita pomoću instalacijskog medija je zaštita kod koje se softver isporučuje najčešće na optičkom mediju, CD-RW ili DVD-RW. Na optičkom mediju se nalazi poseban prostor u kojem se nalazi brojač instalacija programa. Svaki put, nakon uspješno obavljene instalacije, stanje brojača se uveća za jedan[48]. Nakon određenog broja instalacija, više nije moguće instalirati program s određenog medija. Kako bi zaštita bila na razini i kako bi se ona sama ispravno provodila medij mora biti što teže kopirati, a u tu svrhu je potrebno da datoteka s brojačem bude enkriptirana kako bi bilo što teže izmijeniti sadržaj. Danas se taj način zaštite zbog svoje nepraktičnosti vrlo rijetko koristi.

Nekoliko je različitih vrsta zaštite CD medija protiv kopiranja, te svi programi koji se isporučuju na CD mediju imaju takvu zaštitu. Najjosnovniji oblik takve zaštite je provjera da li se ispravan CD nalazi u CD čitaču. Iako je nemoguće razlikovati original od ilegalno kopiranog CD-a, na taj način je moguće spriječiti pokretanje programa s tvrdog diska računala[49]. I najjednostavnijom zaštitom CD medija protiv kopiranja onemogućeno je softverskim piratima da izbace nepotrebne dijelove programa te na taj način smanje prostor koji program zauzima i objave ga na internet. Nešto kompliciranija metoda zaštite protiv

[47] http://www.am.unze.ba/rg/2007/zastita%20digitalnih%20podataka/HTML/dongle.html, 16.08.2014.
[48] http://www.am.unze.ba/rg/2007/zastita%20digitalnih%20podataka/HTML/instalacijski%20mediji.html, 16.08.2014.
[49] http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2004-04-71.pdf, 16.08.2014.

kopiranja CD medija je da se na originalni CD snimi neka informacija koju nije moguće kopirati komercijalno dostupnim softverom za kopiranje CD-a.

Najjednostavniji način zaštite softvera je ugradnja programske funckije koja traži od korisnika unos određene šifre za registraciju[50]. Iako je ta šifra uvijek ista – fiksna registracijska šifra, prednost ove vrste zaštite je u tome što takva šifra nije nužno unesena na disku već se nalazi negdje unutar programskog koda.

Promjenjive registracijske šifre nešto su složeniji način zaštite softvera, a postoje dvije grupe: serijski broj se generira iz korisničkih podataka te serijski broj se generira iz prikupljenih podataka o hardveru računala[51]. Kada je riječ o korisničkim podacima tada se šifra generira na način da se sakupe određeni podaci o korisniku kao što su ime, adresa, naziv poduzeća i slično. u trenutku kada korisnik upiše svoju šifru, program provjerava da li se ona poklapa s izračunatom šifrom. U drugom slučaju se serijski broj generira na osnovu serijskog broja dobivenog uz kupnju softvera i prikupljenih podataka o hardveru, poputkonfiguracije operacijskog sustava, serijskog broja diska i slično. U toku instalacije programa, putem prikupljenih podataka program generira jedinstveni slučajni serijski broj, a aplikacija ga šifrira i skriva u posebnu datoteku. Na taj način prilikom registracije proizvođaču softvera šalje se taj dobiveni identifikacijski kod, a on štalje odgovarajuću šifru potrebnu za instalaciju softvera. Danas se ova vrsta zaštite softvera najčešće koristi, te se uz njega vrlo često koristi zaštita putem interneta.

Serijski broj ovisan o hardveru jedan je od najčešće korištenih načina hardverske zaštite računala. Kada se program instalira generira se pseudo-slučajni serijski broj računala. Pomoću aplikacije taj broj se šifrira i pohranjuje u posebnu datoteku. Kako bi se postigao jedinstveni generirani broj, serijski broj se generira pomoću serijskog broja isporučene kopije softvera te iz prikupljenih podataka o hardveru računala i konfiguraciji operacijskog sustava. Nakon što se program instalira potrebno ga je instalirati, a prilikom instalacije šifra se šalje proizvođaču softvera kojjji korisniku vraća šifru potrebnu za registraciju, a ona odgovara generiranom serijskom broju hardvera.

Zaštita programa pomoću registracijske datoteke ima veliku prednost zbog količine informacija koju je moguće spremiti u njih. Registracijska datoteka u velikoj većini slučajeva

[50] http://security.foi.hr/wiki/index.php/Za%C5%A1tita_programskih_proizvoda, 16.08.2014.
[51] http://www.am.unze.ba/rg/2007/zastita%20digitalnih%20podataka/HTML/registracijske%20sifre.html, 16.08.2014.

enkriptirana te nije moguće pročitati i promijeniti njen sadržaj. U njoj mogu biti pohranjene informacije o korisniku, ključevi za dekriptiranje enkriptiranih dijelova izvršnog koda aplikacije, registracijskoj šifri za autentikaciju korisnika i sl[52]. U tu datoteku također je moguće pohraniti podatke o hardveru korisnikovog računala, upravo iz tog razloga jedinstvena datoteka se koristi za svako računalo.

4.1.3. Programske mjere zaštite

Programske mjere zaštite informacijskog sustava su na razini operacijskog sustava i na razini korisničkih programa. U organizacijama se najčešće koriste višekorisnički operacijski sustavi te je za svakog korisnika potrebno odrediti područje djelovanja i razinu pristupa informacijama što se čini zaštitom pomoću zaporki. Programske mjere zaštite grubo rečeno su sigurnosna pohrana podataka, zaštita od malicioznog softvera i sustavi kriptozaštite. Dalje u radi u kratkim crtama biti će opisana zaštita na razini operacijskog sustava, zaštita na razini korisničke programske podrške, kriptiranje podataka u komunikaciji, antivirus alati, antispyware alati te zaštitni zid odnosno firewall.

Zaštita na razini operacijskog sustava uključuje višekorisnički rad na računalu. Kako bi se zaštitile informacije ovlaštenim informacijama potpuni pristup ima samo administrator, a korisnik ima pristup samo onim informacijama koje mu omogući administrator[53]. U svrhu očuvanja sigurnosti informacija administrator svakom korisniku određuje njegovo korisničko ime te lozinku kojima se koristi kako bi bez problema imao pristup relevantnim informacijama i kako bi obavljao zadatke za koje je zadužen. Sukladno obujmu posla i zadacima za koje je zadužen svaki korisnik zasebno dobiva određenu razinu ovlasti. Svako računalo može imati više administratora te više korisnika, a svi suvremeni operacijski sustavi poput Windows-a, MacOs-a, Linux-a i Unix-a omogućuju upravo ovakvu razinu zaštite.

Zaštita na razini korisničkih programa sljedeći je korak u sigurnosti informacija. U informacijskom sustavo potrebno je ući u određeni korisnički program putem kojega se obavljaju zadaci i aktivnosti vezani uz određenu obavezu prema organizaciji. Korisnički programi štite se kroz tri razine. Prva razina odnosi se isključivo na čitanje podataka iz baze, druga razina omogućuje unos i promijenu podataka u bazi, a treća razina uz sve to omogućuje

[52] http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2004-04-71.pdf, 16.08.2014.
[53] http://www.unizd.hr/Portals/1/Primjena_rac/Poseban_program/Predavanja/sigurnost_predavanje.pdf, 24.08.2014.

i brisanje podataka[54]. Kako bi se osigurala informacijska sigurnost izmjenjeni i brisani podaci ne uklanjaju se na direktan način već se pohranjuju u datoteke kojima ima pristup jedino administrator. Administrator provjerava te podatke i odlučuje da li će se oni uistinu izbrisati ili ne.

Mrežna komunikacija vrlo je osjetljiva i rizična kada je riječ o sigurnosti informacija. Budući da su u suvremenim organizacijama dijelovi poslovnog sustava prostorno dislocirani javlja se potreba za umrežavanjem računala kako bi se informacije mogle zajednički koristiti. Uključivanjem interneta u poslovanje dolazi do pojave novih rizika, a osnovni zahtjevi kojih se treba pridržavati prilikom transfera informacija su osiguranje jednosznačnosti prijenosa te onemogućenje neautoriziranog korištenja ili promjene sadržaja u prijenosu. U mrežnoj komunikaciji najčešće se kao oblik zaštite koristi kriptiranje podataka. Kriptiranje je logička promjena podataka na način da se podatci pošalju primatelju, da nitko drugi osim primatelja i pošiljatelja ne zna izvorne podatke[55]. Kriptiranje funkcionira na temelju šifriranja podataka pomoću određenog ključa i dešifriranja podataka istim ključem. Pošiljatelj šifrira podatke dok primatelj dešifrira ukoliko oboje imaju isti ključ. Na taj način štiti se informacijski sustav na razini mrežne komunikacije.

Računalni virus je računalni program koji može zaraziti druge programe tako da u njih unese kopiju samog sebe, on se može proširiti računalnim sustavom ili mrežom koristeći se ovlastima korisnika koji su zaraženi. Svaki program koji je zaražen postaje virus i tako zaraza raste[56]. Virusi mogu biti i neki drugi štetni programi poput trojanskih konja i crva. Štete koje virusi nanose su osim navedenih i širenje mrežom, krađa korisničkih lozinki, brojeva kreditnih kartica, omogućavanje pristupa neovlaštenim osobama zaraženom računalu i sl. Kako bi se to spriječilo kao zaštita se koriste antivirusni alati. Antivirusni alati sastoje se od nekoliko programa kojima se detektiraju postojeći virusi ili se jednostavno skeniraju datoteke tražeći viruse ili se identificiraju sumnjiva ponašanja od strane kompjuterskog programa koja bi mogla pokrenuti infekciju. Antivirusni alati štite informacijske sustave tako da zaraženu datoteku odvoje od ostalih datoteka kako se virus ne bi širio dalje, brišu zaraženu datoteku ili pokušavaju popraviti datoteku uklanjajući virus unutar iste.

[54] http://www.unizd.hr/Portals/1/Primjena_rac/Poseban_program/Predavanja/sigurnost_predavanje.pdf, 20.08.2014.
[55] http://hr.wikipedia.org/wiki/Kriptografija, 20.08.2014.
[56] http://hr.wikipedia.org/wiki/Ra%C4%8Dunalni_virus#cite_ref-virusi_2-0, 20.08.2014.

Antispyware alati koriste se kako bi se informacijski sustav štitio od spyware-a. Spyware je široka kategorija malicioznog softvera sa namjenom da presreće ili preuzima djelomično kontrolu rada na kompjuteru bez znanja ili dozvole korisnika[57]. U današnje crijeme taj naziv koristi se za široki spektar programa koji koriste korisnikov kompjuter kako bi dobili korisne informacije za neku treću osobu. Kako bi se očuvao informacijski sustav od takvih vrsta ugroza, koriste se antispyware alati ili programi. Antispyware programi djeluju poput antivirusnih programa na način da u trenutku kada je računalo zaraženo reagiraju ili to čine na način da se periodično kontrolira računalo kojim se korisnici u organizaciji koriste. Njima se pregledava Windows Registry, datoteke operativnog sustava i instaliranih programa, kada program uoči datoteku u kojoj se nalazi spyware on je uklanja. Isto tako ako se radi o trenutnom vremenu, prati se tok podataka preko interneta te antispyware programi blokiraju aktivnosti prepoznatih prijetnji.

Da bi određeni program dobio pristup mreži ili računalu organizacije potrebno je dobiti potvrdu firewalla za to. Firewall ili zaštitni zid koristi se kako bi se smanjio rizik zaraze malicioznim kodom te na taj način protok informacija za neovlaštenu upotrebu[58]. Funkcionira na način da pregleda informacije koje dolaze s interneta i odlaze na internet, kada prepozna informacije koje dolaze sa sumnjivih i opasnih lokacija on ih ignorira. Na taj način hakeri koji traže ranjiva računala neće moći vidjeti računalo organizacije ukoliko je zaštitni zid pravilno konfiguriran.

4.2. ORGANIZACIJSKE MJERE ZAŠTITE

Organizacijske mjere su one mjere koje poduzima sam poslovni sustav s ciljem osiguranja željene razine funkcionalnosti sustava te itegriteta podataka u uvjetima djelovanja pretpostavljenih oblika prijetnji. Organizacijskim mjerama smatra se sveukupni sadržaj mjera i postupaka iz oblasti sigurnosti, izrada potrebne dokumentacije koja je potrebna za njihovu primjenu te donošenje i izrada organizacijskih uputa kojima se one provode na radnom mjestu[59].

[57] http://sh.wikipedia.org/wiki/Spyware, 20.08.2014.
[58] http://www.smart.rs/Start/Usluge/Impl/ITbezbednost/Stranice/Firewall.aspx, 20.08.2014.
[59] Šehanović, J., Hutinski Ž., Žugaj M., Informatika za ekonomiste, Tiskara Varteks, 2002, str.237

Postoji nekoliko razina organizacijske sigurnosti na koje je potrebno obratiti pažnju, a to su infrastruktura informacijske sigurnosti, sigurnost pristupa treće osobe te outsourcing. Svaka od tih razina organizacije ima jedinstveni cilj u zaštiti informacijskih sustava.

4.2.1. Infrastruktura informacijske sigurnosti

Cilj infrastrukture informacijske sigurnosti jest upravljati informacijskom sigurnošću unutar organizacije. Drugim riječima kako bi organizacija funkcionirala te da bi se štitile informacije potrebno je poticati multidisciplinarni pristup sigurnosti informacija pravilnom suradnjom od najviših predstavnika u hijerarhiji organizacije do najnižih koji se koriste određenim informacijama. Infrastruktura informacijske sigurnosti može se podijeliti na[60]:

- Tim za upravljanje informacijskom sigurnošću
- Koordinacija rada informacijske sigurnosti
- Dodjela odgovornosti za informacijsku sigurnost
- Proces autorizacije organizacijskih cjelina koje sudjeluju u obradi
- Savjeti specijalista o informacijskoj sigurnosti
- Suradnja između organizacija
- Neovisni pregledi efikasnosti informacijske sigurnosti

Svi članovi managerskog tima moraju se brinuti za informacijsku sigurnost jer je to njihova poslovna odgovornost. Tim za upravljanje informacijskom sigurnošću osniva se kako bi se lakše obavljali poslovi sigurnosti informacija u organizaciji, a jedan manager je odgovoran za sve aktivnosti koje su vezane uz sigurnost počevši od pregleda i odobravanja politike informacijske sigurnosti, praćenja promjena koje mogu prijetiti informacijskoj imovini pa sve do praćenja incidenata te odobravanja postupaka kojima se postiže poboljšanje informacijske sigurnosti.

Koordinacija rada informacijske sigurnosti najpotrebnija je u organizacijama koje su velike pa se kroz tim predstavnika managera relevantinh dijelova organizacije vrše radnje vezane uz koordinaciju. To je su najčešće: dogovaranje specifičnih uloga i određenih odgovornosti za informacijsku sigurnost za cijelu organizaciju., koordiniranje i podržavanje inicijative vezane uz informacijsku sigurnost, pregled izvješća o sigurnosnim incidentima,

[60] http://es.scribd.com/doc/17094401/50/Kontrola-pristupa, 19.08.2014.

te općenito radnje vezane uz očuvanje sigurnosti informacija na razini cjelokupne organizacije.

Politika informacijske sigurnost treba pružiti općenito vodstvo za dodjelu sigurnosnih uloga i odgovornosti u organizaciji[61]. Gavni cilj jest da su sve odgovornosti informacijske sigurnosti jasno određene. Iz tog razloga najveća pažnja se usmjerava na identifikaciju i jasno definiranje dijelova imovine te sigurnosnih procesa pridruženih svakom pojedinom sustavu, zatim treba odrediti tko je odgovoran za pojedini dio imovine ili sigurnosni proces te jetaj dogovor potrebno dokumentirati. U kunačnici je potrebno dokumentirati te definirati razine ovlasti.

Proces autorizacije organizacijskih cjelina koje susjeluju u obradi bitan je kada se uvodi novi organizacijski dio u poslovanje, tada manageri zaduženi za informacijsku isgurnost moraju autorizirati namjenu i korištenje tog dijela organizacije, trebaju se provoditi kontrole hardvera i softvera posebice ako se za rad koriste osobna računala gdje je potrebno kontrolirati i autorizirati rad jer primjena osobnih računala može biti vid ranjivosti organizacije.

Svaka organizacija trebala bi imati i određene specijaliste koji će davati savjete za informacijsku sigurnost. Specijalisti informacijske sigurnosti posjeduju uravnotežene analitičke vještine i poslovnu sposobnost[62]. Njihova uloga je provoditi kontrolu informacija i sigurnosti protoka informacija, te kada je to potrebno provoditi istrage, mjere i kontrole potrebne da se očuva informacijska sigurnost. Sve organizacije nemaju svoje savjetnike za informacijsku sigurnost pa tu ulogu preuzima osoba koja je najviše upoznata sa stanjem u organizaciji i njenim radom.

Kada je riječ o suradnji među organizacijama u ulozi informacijske sigurnosti potrebno je ograničiti razmjenu informacija kako se ne bi dogodilo da one dođu do neovlaštenih osoba. Suradnja je bitna sa zakonodavnim i koordinativnim tijelima, pružateljima informacijskih usluga te telekomunikacijskih operatera[63].

Neovisni pregledi efikasnosti informacijske sigurnosti bitni su kako bi se utvrdilo vrši li se pravilno sigurnosna politika u organizaciji. Za takve preglede zadužena je unutarnja nadzorna funkcija, neovisni manager ili vanjska organizacija koja je specijalizirana za takve

[61] http://os2.zemris.fer.hr/ISMS/2008_kovacevic/primjerSP_2.html, 19.08.2014.
[62] https://www.fer.unizg.hr/poslijediplomski/specijalisticki_studij/informacijska_sigurnost, 19.08.2014.
[63] http://www.scribd.com/doc/17094401/13/suradnja-izme%C4%91u-organizacija, 19.08.2014

preglede i čiji članovi posjeduju potrebne vještine i iskustva[64]. Uloga osoba zaduženih za kontrolu je pregledavanje implementacije dokumenata o politici informacijske sigurnosti te odgovornosti za istu.

4.2.2. Sigurnost pristupa treće zainteresirane strane

Kada je za potrebe poslovanja potrebno uključiti i treće osobe logično je da će organizacija uključiti posebne mehanizme kontrole kako bi se održala potrebna razina sigurnosti organizacijskih jedinica. Kako bi se osigurala sigurnost informacija koriste se i procjene rizika te se kontrolni mehanizmi ugovaraju s trećom stranom koja ima doticaj s informacijama.

Kod pristupa danog trećoj strani bitno je razlikovati i identificirati rizik koji se pojavljuje kod tog pristupa. Postoje dvije vrste pristupa: fizički te logički pristup[65]. Fizičkim pristupom omogućava se trećim stranama pristup uredima, prostorijama s računalnom opremom i ormarima za pohranu, dok se logički pristup odnosi na pristup bazama podataka štićene organizacije te informacijskim sustavima.

Radi vrste i obujma poslovanja organizacije treće strane dobivaju pristup informacijama. Omogućavanjem pristupa informacijama treće strane u dogovoru s organizacijom pristaju na kontrolne mehanizme koje će provoditi organizacija kako bi se smanjio rizik neovlaštenih upotreba informacija. Tek kada se potpiše ugovor treće strane mogu dobiti potrebne informacije potrebne za rad.

Treće strane mogu biti čistači, dobavljači, zaštitari, usluge omogućene kroz outsourcing, privremeno zaposleni studenti, razni konzultanti, osoblje koje se brine o hardveru i softveru, partneri i sl.

4.2.3. Outsourcing

Outsourcing se može definirati kao korištenje vanjskih poduzeća i pojedinaca za obavljanje pojedinog posla[66]. Sukladno s definicijom outsourcinga, cilj organizacije je održati sigurnost informacija u slučaju kada je obrada istih povjerena nekoj drugoj organizaciji.

---

[64] http://www.scribd.com/doc/17094401/47/Upravljanje-mre%C5%BEom, 19.08.2014.
[65] http://os2.zemris.fer.hr/ISMS/2008_kovacevic/primjerSP_2.html, 19.08.2014.
[66] http://www.moj-posao.net/Vijest/60807/Outsourcing-sto-je-i-zasto-se-koristi/, 20.08.2014.

Kada se ugovara posao outsourcing-a bitno je kao i s ostalim trećim stranama sklopiti neku vrstu ugovora kojim se kontrolni mehanizmi, procjena rizika i sigurnosni postupcim provode kako bi se spriječilo neovlašteno korištenje informacija u organizaciji. Ugovorom o outsourcing-u zadani su određeni uvjeti odnosno zahtjevi kojih se treba držati prilikom obavljanja određenog posla za organizaciju. Stavke koje takav ugovor može sadržavati su[67]:

- Načini kojim se udovoljava zakonskim rješenjima
- Vrste sporazuma koji se ugovaraju kako bi obje strane bile svjesne svojih sigurnosnih odgovornosti
- Načini na koje se provjerava i održava integritet te povjerljivost poslovne imovine
- Fizičke i logičke kontrole kojima se organizacija koristi kako bi ograničila pristup informacijama koje su dostupne samo ovlaštenim korisnicima
- Načini dostupnosti podataka u slučaju katastrofe
- Razina fizičke sigurnosti primjenjiva na opremu danu u outsourcing-u
- Pravo na nadzor

Glavna prednost outsourcinga je da se organizacija može usredotočiti na svoju osnovnu aktivnost dok i razvoj poslovnih procesa, jer su sporedni poslovi dani drugoj organizaciji koja obavlja to za njih. Naravno da je u ovakvom obliku rješavanja poslova potrebna itekako visoka razina kontrole i zaštite informacijskih sustava.

4.3. FIZIČKE MJERE ZAŠTITE

Fizičke mjere zaštite se uz ostale mjere zaštite koriste kako bi se očuvala sigurnost informacijskih sustava. Fizička sigurnost ugrožava se u slučajevima elementarnih nepogoda, poplave, potresa i požara te ljudskih ranjivosti, kao što je sabotaža, krađa i neposlušnost. Primjena fizičke sigurnosti podrazumijeva proces uporabe mjera zaštite kako bi se spriječio neovlašten pristup, oštećenje ili uništenje dobara[68]. Fizička sigurnost može se smatrati osnovom informacijske sigurnosti te su ostale sigurnosne mjere utemeljene upravo na njoj. Cilj fizičke sigurnosti je spriječiti neautorizirane pristupe računalnom sustavu, zaštititi

[67] http://www.scribd.com/doc/17094401/Sigurnost-informacijskih-sustava, 20.08.2014.
[68] (http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-06-304.pdf, 30.08.2014.).

integritet podataka koji se pohranjuju na računalo, u slučaju raznih nepogoda spriječiti oštećenje ili gubitak podataka te spriječiti krađu podataka s računalnih sustava.

4.3.1. Prijetnje fizičkoj sigurnosti

Da bi se odredile mjere zaštite informacijskih sustava potrebno je navesti koje su sve prijetnje koje tu sigurnost ugrožavaju. Nekoliko je grupa prijetnji koje će biti opisane u daljnjem teksu, a to su: prirodne nepogode, ljudske prijetnje i ostale prijetnje.

Prirodne nepogode su prva kategorija prijetnji fizičkoj sigurnosti, a karakteristika im je na na takve prijetnje čovjek ne može utjecati. Budući da će se prirodne nepogode dogoditi u svakom slučaju, uloga čovjeka je određenim mjerama spriječiti gubitak informacija potrebnih za poslovanje te općenito omogućiti nastavak neprekidnog rada informacijskog sustava. U skupinu prijetnji fizičkoj sigurnosti u vidu prirodnih nepogoda ubrajamo[69]:

- Meteorološke nepogode – razne padaline, vjetar, oluja jako niske ili visoke temperature na informacijski sustav mogu djelovati tako da se izgubi ili degradira komunikacija te uništenje samih uređaja gdje informacije mogu biti pohranjene
- Geofizičke nepogode – potresi i vulkanske aktivnosti izazivaju požare, poplave, ispuštanje raznih štetnih tvari, kemikalija i plinova te dolazi do prekida napajanja.kao i kod meteoroloških nepogoda i kod goefizičkih nepogoda jednake su prijetnje i rizici.
- Sezonski fenomeni – uništenje uređaja ili gubitak te degradacija mrežnih komunikacija mogu biti uzrokovani i ekstremnim vremenom kao što su uragani, šumski požari i slično.
- Astrofizički fenomeni – utjecaj sunčanih fenomena te meteora također može dovesti do gubitka ili degradacije satelitskih veza te time naštetiti sigurnosti informacijsih sustava.
- Biološke snage – radna snaga je potrebna za očuvanje informacijskog sustava, a razne bolesti mogu uzrokovati smanjenje broja sposobne radne snage za obavljanje određenog posla.

Druga kategorija prijetnji su ljudske prijetnje jer upravo zaposlenici, korisnici, klijenti, poslovni partneri, dobavljači i ostale osobe koje imaju doticaj s imovinom i podacima

[69] http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-06-304.pdf, 30.08.2014.

organizacije čine informacijsku sigurnost ranjivom svojim namjernim ili slučajnim potezima. Zaposlenici uzrokuju razne prijetnje, a one su[70]:

- Neposlušnost – ona dovodi do prosvjeda ili štrajka te u takvim situacijama može doći do oštećenja opreme i uređaja potrebnih za rad ali se isto tako mogu ozlijediti sami zaposlenici.
- Otkrivanje osjetljivih podataka – zbog nepravilnog rukovanja ili zbog nepoštivanja sigurnosne politike organizacije.
- Sabotaža – predstavlja namjerno narušavanje rada sustava i ispravnosti uređaja te je potrebno uvesti mjere kako bi se taj čin spriječio
- Nenamjerno oštećenje imovine – nepravilno i nedovoljno educirani zaposlenici mogu oštetiti uređaje ili dio neke druge imovine, pa je stoga potrebno poraditi na njihovoj edukaciji da bi se takve prijetnje mosle svesti na minimum
- Zlouporaba ovlasti – javlja se kada se zaposlenici ne pridržavaju pravila poslovanja i svojih ovlasti, može se dogoditi da prekomjereno koriste imovinu organizacije ili istu iznose van prostora za koji nije namjenjena
- Neovlašten pristup podacima ili imovini – zaposlenik mora prema ugovoru o povjerenju poštivati upotrebu povjerljivih informacija
- Krađa – zaposlenik namjerno otuđuje dio imovine organizacije

Osim ljudskih prijetnji i prirodnih nepogoda postoje i ostale prijetnje fizičkoj sigurnosti izazvane nekim nesrećama. Takve nesreće mogu biti razne eksplozije, prašina, gubitak električnog napajanja, elektromagnetska radijacija, poplave uzrokovane nekim kvarom. U svakom slučaju sve prijetnje mogu prouzročiti velike gubitke, stoga je potrebno uspostaviti određene mjere zaštite kojima će se informacijski sustavi zaštititi.

4.3.2. Područja zaštite

Radi li se o fizičkoj zaštiti informacijskih sustava tada je potrebno štititi ne samo pojedino mjesto na kojem se povjerljive informacije nalaze, već i cijelu okolinu kako bi što teže bilo doprijeti do određenih informacija. U tu svrhu postoji zaštita okoline, zaštita recepcije, zaštita prostorija, zaštita same opreme zatim kontrola pristupa i sl.

[70] http://security.lss.hr/arhiva-dokumenata/fizicka-sigurnost-informacijskog-sustava.html, 31.08.2014.

Zaštita okoline od prvi je korak koji treba poduzeti kada se štiti informacijski sustav. Najšire gledano ukoliko se ne može ući u određeni prostor gdje se informacija nalazi nije moguće ni ugroziti sigurnost informacijskog sustava. Kada je riječ o fizičkoj zaštiti tada u svrhu očuvanja informacijskog sustava postoje ograde ili zidovi koji štite okolinu organizacije te time brane pristup i uvid u ono što se događa u samoj organizaciji. Najbitniji dio te tog područja su ulazi i izlazi koje je potrebno više nagledati pomoću kamera, postavljanja lokota tako da pristup imaju samo osobe s ključem te postaviti zaštitare kako bi se utvrdilo tko ima pristup, a tko ne. Kao preventiva kriminalitetu i radi sigurnosti informacija okolina se štiti kroz CDTED dizajn (Crime prevention through environmental design) koji predstavlja multidisciplinarni pristup odvraćanja kriminalnog ponašanja kroz dizajn okoliša[71]. Dizajnom okoliša daje se do znanja što spada u javno, a što u privatno vlasništvo te je na taj način lakše identificirati sumnjive prijestupnike.

Kod većine organizacija na samom ulasku u objekt nalazi se neka vrsta recepcije odnosno mjesto na kojem se obavljaju određeni administrativni poslovi te gdje je moguće dobiti razne informacije. Rad na recepciji potrebno je kontrolirati na način da važni dokumenti ne stoje na vidiljvim mjestima dostupnim svima koji se nalaze u objektu, zatim je potrebno zaštititi rad na računalu tako da je usmjeren da klijent ne vidi što zaposlenik radi na njemu i slično. Osim ove vrste fizičke zaštite informacija na recepciji moguće je postaviti i kamere kako bi se vršio bolji nadzor, razne prekidače za slučaj opasnosti te alarme. Zaposlenik također mora paziti na svoj rad i ne napuštati radno mjesto dok nije spremio povjerljive informacije na za to predviđeno mjesto i onesposobio rad za neovlaštene osobe.

Prostorije sa skupocjenom opremom ili važnim poslužiteljima također treba zaštititi u skladu s namjenom informacija u tim prostorijama. Najčešće se to radi na način da su postavljene kamere, protupožarni i protuprovalni alarmi, razni prekidači za zaposlenike u slučaju opasnosti te općenito implementacijom sustava protiv neovlaštenog ulaska u određenu prostoriju.

Zaštita opreme smatra se najvažnijim aspektom fizičke zaštite informacijskog sustava, ali joj nije usmjerena dovoljna pažnja u obliku načina zaštite. Radi se o tome da se svaka oprema odnosno uređaj vrednuje po svojim karakteristikama i namjeni stoga je razina zaštite različita za različiti uređaj ili opremu. Većinom ta zaštita podrazumijeva samo zaštitu primjerice osobnog računala na kojem zaposlenik radi ili zaštitu poslužitelja no potrebno je

[71] http://en.wikipedia.org/wiki/Crime_prevention_through_environmental_design, 31.08.2014.

obratiti pažnju i na ostalu opremu. Primjerice staviti prijenosne medije s informacijama na sigurno mjeso, uništavanje starih medija na pravilan i siguran način, zaključavanje uređaja i sl.

Kontrola pristupa važna je kada je riječ o fizičkoj zaštiti informacija. Nju karakterizira nemogućnost ulaska u objekt osobama koje nemaju odobrenje za to. Najčešće se primjenjuje kontrola pristupa na način da se zaposle zaštitari ili druge osobe koje će kontrolirati tko ima pristup, a tko ne. Osim tog načina kontrola pristupa provodi se putem mehaničkih sredstva i tehničkih sredstva[72]. Kontrola pristupa nije ista za zaposlenike i korisnike u organizaciji stoga se za svakog posebno određuje koje su im ovlasti. Najčešće se na samom ulazu u objekt identificiraju korisnici i posjetitelji kako bi se umanjila mogućnost zlouporabe pristupa unutrašnjosti objekta ili nekim dijelovima informacijskih sustava. postoje mnogi načini na koje se kontrola pristupa provodi a u suvremeno doba to se pametne kartice za kontrolu pristupa, skeniranje otiska prsta, šarenice oka ili pak prepoznavanje glasa.

Navedena područja fizičke zaštite informacijskih sustava kontroliraju se i pomoću EPS (electronic physical security). EPS je integrirana primjena brojnih elektroničkih sustava za sigurnost kao što su[73]: sustavi za detekciju požara, automatski sustavi za suzbijanje plinova, sustavi za nadzor, sustavi za kontrolu pristupa, sustavi za detekciju upada, adekvatna oprema za zaštitare te sustavi za opremanje okoline i prostorija.

4.3.3. Elementi za postizanje fizičke sigurnosti

Prethodno u radu su navedene prijetnje fizičkoj sigurnosti informacija te područja koja se štite kada je rič o sigurnosti informacijskih sustava. U ovom dijelu rada biti će opisani elementi koji se koriste za postizanje fizičke sigurnosti od alarmnih sustava, rasvjete, zaštitara, nadzornih kamera, uređaja za kontrolu pristupa, sustava za zaključavanje prostorija i opreme te sustava za praćenje i otkrivanje lokacije.

Kako bi se upozorilo korisnike i zaposlenike u organizaciji o nekom nastalom problemu koriste se alarmni sustavi. Alarmnim sustavima daju se vizualna ili zvučna upozorenja o

[72] http://www.alarmautomatika.com/idea-project/document/09028-rjesenja-kontrole-pristupa-i-evidencije-radnog-vremena.pdf, 31.08.2014.
[73] http://books.google.hr/books?id=hbQIAAAAQBAJ&pg=SA1-PA19&lpg=SA1-PA19&dq=eps+electronic+physical+security&source=bl&ots=aRKzXXSs9f&sig=qNg6b738bpu58WYyCfR63fMBLlY&hl=hr&sa=X&ei=FZEEVLCIB4fmyQPT2ILgBw&ved=0CBoQ6AEwAA#v=onepage&q=eps%20electronic%20physical%20security&f=false, 31.08.02014.

stanju sustava ili novonastalom problemu. Alarmnih sustava ima nekoliko vrsta ovisno o namjeni[74]:

- Alarmi za sigurnost - alarmi za dojavu prirodnih nepogoda i izvanrednih situacija poput radijacije
- Alarmi u Q&M sustavima (operation and maintenance) – služe za slanje obavijesti o lošem radnom stanju sustava kojeg nadzire
- DCS sustavi(distributed control manufactoring system) –obavještavaju osoblje o važnim događajima, najčešće se lprooste u kemijskim i nuklearnim labaratorijima
- Vremenski alarmi – aktiviraju se u trenutku kada je to odredila osoba koja ga je aktivirala
- Alarmi protiv provala – u slučaju provale pomoću njih obavještava se policija, najčešće su to tihi alarmi da ne bi zbunili provalnika.

Važnost alarma je vrlo velika kada je riječ o zaštiti informacijskih sustava jer se upotrebom alarma pravovremeno detektiraju uljezi i reagira se u trenutku. Negativna strana alarma je to što je moguće da se aktiviraju i kada za to nema potrebe. Primjerice protupožarni alarmi aktiviraju se detekcijom dima. Dim se može stvoriti i pušenjem cigarete i ako se protupožarni alarm nalazi u blizini i detektira dim može zaključiti da prijeti požar, a to zapravo nije slučaj. U svakom slučaju pravovremeno reagiranje alarma dovodi do toga da se pravovremeno informacije štite i time omogućava očuvaje sigurnosti informacijskog sustava.

U svrhu podizanja fizičke sigurnosti informacija može se koristiti i rasvjeta. Rasvjeta omogućava preglednost prostora i pruža sigurnost korisnicima i zaposlenicima u organizaciji. Rasvjeta može biti periodična, odnosno konstantna na način da se pali u zadanom vremenskom intervalu i gasi preko dana primjerice. Na taj način se omogućava drugim elementima fizičke zaštite – alarmima da svoju ulogu obavljaju besprijekorno. Osim određenih vremenskih intervala kada je rasvjeta uključena, postoji i aktiviranje i deaktiviranje rasvjete putem senzora te se na taj način štedi elekrična energija.

Elementi fizičke zaštite informacijskih sustava su već spominjani zaštitari. Zaštitari su posebno obučeni zaposlenici koji su educirani za pružanje zaštite vlasništva, dobra i osoba neke organizacije. Posao zaštitara je spriječiti bilo koje radnje vezane uz kriminal i općenito štititi organizaciju od opasnih radnji. Prilikom zapošljavanja zaštitari najčešće prolaze

[74] http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-06-304.pdf, 31.08.2014.

određene testove kojima se mjere njihove sposobnosti i sukladno vrsti posla njihove reakcije. Zapošljavanjem zaštitara uvelike se pospješuje sigurnost informacijskih sustava jer svojim prisutstvom zaštitar ulaže povjerenje zaposlenicima te strah razbojnicima. Njegova uloga je patrolirati, obilaziti objekte kako bi se uvjerio da nema prijetnji, zatim provoditi kontrolu na ulazu u objekt te pravilno reagirati u slučaju opasnosti kako bi očuvao i zaštitio informacijski sustav.

Nadzorne kamere još su jedan element fizičke zaštite informacijskih sustava. Njima se kontrolira određeno stanje u organizaciji, oprema, uređaji, zaposlenici i slično. Nadzornih kamera ima nekoliko vrsta te namjena istih ovisi o tome što se nadzire i koliko je potrebno određenu poslovu situaciju i objekt štititi. Bez obzira o kojoj vrsti nadzornih kamera je riječ one održavaju fizičku sigurnost tako da[75]:

- Sprječavaju zločine
- Omogućavaju praćenje prijevoza opreme
- Pružaju mogućnost kontrole prilaska objektima
- Omogućuju identifikaciju osoba na ulazu
- Omogućuju praćenje aktivnosti zaposlenika i posjetitelja

Danas se najviše koriste IP (Internet Protocol) nadzorne kamere, koje se omogućuju preko internetske veze te je moguć stalni pregled stanja u organizaciji gdje su kamere postavljene.

Uređaji za kontrolu pristupa jedni su od važnijih zaštita pristupa objektu, tj. dozvole pristupa (ulaza/izlaza) ovlaštenim osobama ili zaposlenicima[76]. U današnje vrijeme postoji nekoliko načina na koje se kontrolira pristup i time štite informacije. Pristup se može kontrolirati putem pametnih kartica za identifikaciju korisnika i zaposlenika, zatim identificiranjem osobe kroz otisak prsta, šarenicu oka, glas ili crte lica. Prema načinu na koji se korisnik sustava identificira razlikuju se fizičko i ponašajno prepoznavanje. Fizičko prepoznavanje odnosi se na oblik tijela, otisak prsta, prepoznavanje lica, geometriju ruke, šarenice oka i sl. Ponašajno identificiranje odnosi se na ritam, hod ili boju glasa zaposlenih ili korisnika.

Kako bi se fizički osigurala neka prostorija najčešće se koriste sustavi za zaključavanje prostorija da bi informacijski sustav ostao netaknut i siguran. Sustavi za zaključavanje su

[75] http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-06-304.pdf, 31.08.2014.
[76] http://www.aam-mihalinec.hr/kontrola-pristupa.php, 31.08.2014

mehanički ili elektronički uređaji u funkciji lokota. Prostorije se ovisno o razini zaštite zaključavaju pomoću ključa, kartica, lozinki ili njihovom kombinacijom. Osnovna namjena sustava za zaključavanje je spječavanje fizičkog pristupa nekom dobru ili imovini, a mogu se koristiti na vratima, prozorima, ormarićima ili uređajima[77]. Prijetnje koje se javljaju kad je ovaj element u funkciji zaštite su provale, no uz odgovarajuću kombinaciju s alarmima ili primjenom elektroničkog lokota otežava se razbojništvo te se čuva sigurnost informacija.

Uz uređaje za zaključavanje prostorija postoje i uređaji za zaključavanje opreme. Baš kao i uređaja za zaključavaje prostorija i uređaja za zaključavanje opreme ima nekoliko vrsta od onih koji omogućuju fizičko zaključavanje kabela do onih koji ne zahtjevaju nikakve posebne utore na uređaju te u konačnici elektronička rješenja koja sadrže i alarmne sustave. Dakle postoji sistem koji se koristi za spajanje uređaja za zaključavanje kabela. Obično se na metalnom kablu nalazi neka vrsta lokota koja se ključem ili određenom kombinacijom može otvoriti. Bez ključa ili kombinacije ne može se kabel izvaditi prisilno te ostaje vidljiv trag namjere za otuđivanjem uređaja, pa time i informacija koje se nalaze na njemu. Osim putem kabla, alternativa su i mehanizmi zaključavanja za koje nije potreban poseban utor, pa se to čini primjerice preko priključka za pisač te imaju posebne vijke za osiguravanje na mjestu[78]. Nešto nezgodniji način zaključavanja prijenosnog računala je s držačima koji sadrže neku vrstu lokota, a obuhvaćaju cijelo računalo te su pričvršćeni za nepomički objekt. Najjednostavni način na koji se zaključava oprema je putem pohranjivanja u za to predviđene ormariće.

Sustavi za praćenje i otkrivanje lokacije nešto su sofisticiraniji od prethodno spomenutih elemenata za postizanje fizičke sigurnosti. Budući da se u uređajima poput prijenosnih računala ili raznih drugih prijenosnih medija nalazi velika količina povjerljivih informacija bitno je dobro paziti na njihovu sigurnost. S obzirom da bi šteta bila puno veća od one materijalne prirode, razni uređaji koji se koriste u poslovanju organizacije osigurani su na način da su u njih ugrađeni sustavi za praćenje i otkrivanje lokacije, a uloga im je detektirati krađu te otkriti položaj ukradenog uređaja ili druge opreme[79]. Većina sustava za praćenje i otkrivanje lokacije funkcionira na principu internetske veze. Kada se prijavi krađa, ukoliko na prijenosnom računalu postoji takav sustav i ako je računalo u funkciji te na internetu, vlasniku/korisniku prijenosnog računala stižu podaci o tome gdje je računalo locirano, slike

[77] http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-06-304.pdf, 31.08.2014.
[78] http://www.condorsecuritybih.com/#!noviteti-najnovije-opreme-na-titu/chbg, 31.08.2014.
[79] http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-06-304.pdf, 31.08.2014.

osobe koja trenutno koristi otuđen uređaj, te se provodi tzv. tajno šifriranje svih podataka koje korisnik prethodno označi za tu namjenu. Ovisno o sustavu koji je ugrađen u otuđen uređaj razlikovati će se i povratne informacije koje dobiva korisnik o lokaciji svog uređaja.

Sve vrste zaštite informacijskih sustava jako su važne za očuvanje informacija, te nije dovoljno da se provodi samo jedna vrsta zaštite, već je potrebno koristiti kombinaciju fizičkih, organizacijskih, softversko – hardverskih mjera zaštite informacijsih sustava. suvremena poduzeća prepoznaju tu važnost te u svrhu učinkovitosti poslovanja te veće konkurentnosti koriste što veći broj mjera zaštite informacija u raznim kombinacijama ovisno o djelatnosti koju određena organizacija obavlja.

5. PRIMJERI IZ POSLOVNE PRAKSE

U prethodnim poglavljima ovoga rada dan je pregled teoretskog dijela vezanog uz sigurnost informacijskih sustava. Kako bi se prikazala kompletna slika postojećeg stanja u Republici Hrvatskoj vezanog uz temu ovog diplomskog rada primjeniti će se anketa s nekoliko konkretnih pitanja te će se analizirati svjesnost ljudi o potrebama zaštite informacijskog sustava u organizacijama u kojima rade. Ovo poglavlje sastoji se od dva dijela. U prvom dijelu biti će prikazan izgled ankete, odnosno biti će navedena pitanja na koja su odgovarali ispitanici, a sukladno tim pitanjima u slijedećem dijelu biti će prikazana analiza prikupljenih anketa. Anketa je provedena na pedeset ispitanika iz raznih područja djelovanja, pa je na taj način prikazana realna situacija na razini države.

5.1. SADRŽAJ ANKETE O SIGURNOSTI INFORMACIJSKIH SUSTAVA

Anketa s nazivom Sigurnost informacijskih sustava sastoji se od osam kratkih i konkretnih pitanja različitih formi. Cilj ove ankete je prepoznati važnost i ulogu mjera zaštite informacijskih sustava u današnjosti, te svjesnost i informiranost vlasnika, zaposlenih i korisnika neke organizacije o ovom problemu. Anketa je provedena na uzorku od 50 nasumičnih ispitanika iz raznih područja poslovanja neke organizacije. S obzirom da je anketa anonimna, nije moguće konkretno reći o kojim je poduzećima riječ, no u analizi ankete postoji dio koji se oslanja na djelatnost organizacije u kojoj je ispitanik zaposlen. Originalna pitanja korištena u anketi su sljedeća:

Prva dva pitanja ove ankete sastoje se od pitanja i odgovora koji se nadopisuju ovisno o ispitaniku i njegovom položaju u organizaciji.

1.Kojom se djelatnošću bavi poduzeće u kojem ste zaposleni?_____.

2.Koja je vaša uloga u poduzeću (vlasnik, zaposlenik, menadžer...)?_____.

Slijedeća pitanja prikazuju svjesnost ispitanika o zakonskoj regulativi vezanoj za sigurnost informacijskih sustava, forma prvih dva pitanja ovog dijela ankete je pitanje s višestrukim odabirom odgovora, dok je treće pitanje „da-ne“pitanje.

3.Prepoznajete li po imenu ili znate nešto o nekoj od ovih institucija koje se brinu o informacijskoj sigurnosti u Hrvatskoj:

- Nacionalni CERT
- Zavod za sigurnost informacijskih sustava
- Ured vijeća za nacionalnu sigurnost
- Agencija za podršku informacijskim sustavima i informacijskim tehnologijama
- Agencija za zaštitu osobnih podataka
- Središnji državni ured za e-Hrvatsku
- Sve institucije su mi poznate
- Nijedna institucija mi ne zvuči poznato

4.Označite zakone o informacijskoj sigurnosti koji su Vam poznati ili znate nešto o njima:

- Zakon o informacijskoj sigurnosti
- Zakon o zaštiti osobnih podataka
- Zakon o sigurnosno-obavještajnom sustavu RH
- Zakon o elektroničkoj ispravi
- Svi zakoni su mi poznati
- Nijedan zakon mi nije poznat

5.Jeste li znali da su norme ISO 27001 (Sustav upravljanja informatičkom sigurnošću) te ISO 27002 (Kodeks postupaka za upravljanje sustava informacijske sigurnosti) od velike važnosti za informacijsku sigurnost kako na međunarodnoj razini tako i na razini Republike Hrvatske?

- DA
- NE

Slijedeće pitanje postavlja se ispitanicima da bi se dobilo njihovo mišljenje o informatizaciji poslovanja i njezinoj ulozi u sigurnosti informacijskih sustava, više je ponuđenih odgovora, a moguće je odabrati samo jedan. Pitanje glasi:

6.U suvremeno doba, smatrate li da uspješno funkcioniranje i sigurnost informacijskih sustava ovisi o tome da li je takav sustav podržan računalom?

- Da, u potpunosti se slažem da je potrebna upotreba računala kako bi se održala sigurnost informacijskih sustava

- Ne, kako bi informacijski sustav pravilo funkcionirao nije potrebna upotreba računala
- Smatram da informacijski sustav može biti jednako uspješan ako je ili nije podržan računalom, ovisno koju djelatnost organizacija obavlja
- Ne mogu se odlučiti za niti jedan od ponuđenih odgovora

Slijedeće pitanje odnosi se na mišljenje ispitanika o tome koje mjere zaštite su najbitnije u poslovanju. Forma pitanja jest više ponuđenih odgovora s mogućnošću odabira jednog odgovarajućeg.

7.Za zaštitu informacijskih sustava i uspješno poslovanje organizacije potrebno je koristiti:

- Samo fizičku zaštitu informacija (alarmi, nadzorne kamere, zaštitari, kontrola pristupa i sl.)
- Samo hardversko-softversku zaštitu informacija (autorska prava, šifre za registraciju, antivirusni programi, firewall, kriptiranje podataka i sl.)
- Samo administrativno-organizacijska zaštita informacija (podjela uloga i ovlaštenja, administrator-korisnik i sl.)
- Kombinacija prethodno navedenih mjera zaštite je najbolja opcija za sigurnost informacijskih sustava

U konačnici za kraj ankete postavljena je hipoteza koju je potrebno dokazati u diplomskom radu, te se od ispitanika traži da odgovore slažu li se s njom ili ne.

8.Slažete li se s navedenom tvrdnjom: „Sigurnost informacijskih sustava pomaže pri rješavanju određenih problema vezanih uz osiguranje kontinuiteta poslovanja te upravljanje sigurnošću informacija u suvremenim organizacijama.“

- Da, slažem se s postavljenom tvrdnjom.
- Ne, ne slažem se s postavljenom tvrdnjom.

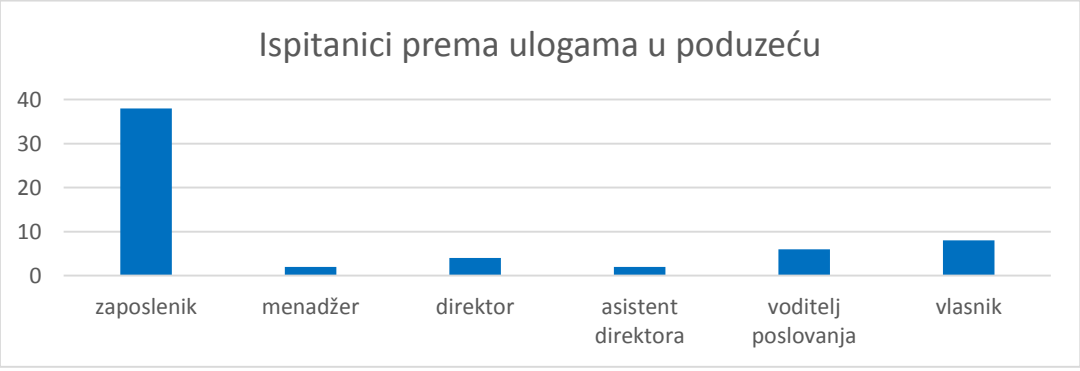
5.2. ANALIZA ANKETE O SIGURNOSTI INFORMACIJSKIH SUSTAVA

Anketa navedena u prethodnom potpoglavlju provedena je na pedeset nasumičnih ispitanika. Rezultati ankete prikazuju realno stanje informiranosti ljudi o informacijskoj sigurnosti, zakonima te značaju zaštite informacija. Ispitanici koji su rješavali anketu obavljaju različite djelatnosti te se nalaze na različitim pozicijama u nekoj organizaciji stoga je dan kompletan pregled stanja u državi. Budući da je anketa jako sažeta i cilj joj je bio u kratkim crtama prikazati realno stanje u državi, rezultati će biti prikazani putem raznih grafikona te analizirani na prikladan način.

Prva dva pitanja ankete odaju nam tko su zapravo ispitanici, njihova uloga u organizaciji i djelatnost kojom se bave. Prema rezultatima ankete ispitanika ima iz javnih institucija, uslužnih te proizvodnih djelatnosti. Budući da se podosta razlikuju djelatnosti kojima se ispitanici bave, biti će navedeno samo nekoliko njih. Dakle prema rezultatima ankete, mišljenje o stanju sigurnosti informacijskih sustava u državi dobiveno je iz ovih područja poslovanja: marketing i menadžment, IT, telekomunikacije, MORH, knjižničarska djelatnost, turizam, sport, poljoprivredna djelatnost, istraživanje i razvoj, pomorstvo i promet, prodaja i iznajmljivanje nekretnina te mnogo drugih.

S obzirom da svjesnost samo vlasnika ili menadžera, direktora te ostalih zaposlenih u organizaciji na višim razinama nije dovoljna kako bi se održala sigurnost informacija koje se nalaze unutar neke organizacije potrebno je ispitati apsolutno sve koji imaju doticaj s organizacijom. Za potrebe ove ankete najviše ispitanika su "obični" zaposlenici, koji bi itekako trebali biti informirani te upoznati sa očuvanjem sigurnosti informacija u svojoj organizaciji. Na grafikonu 1. prikazan je sastav ispitanika koji su odgovarali na anketu.

Grafikon 1. Ispitanici prema ulogama u poduzeću

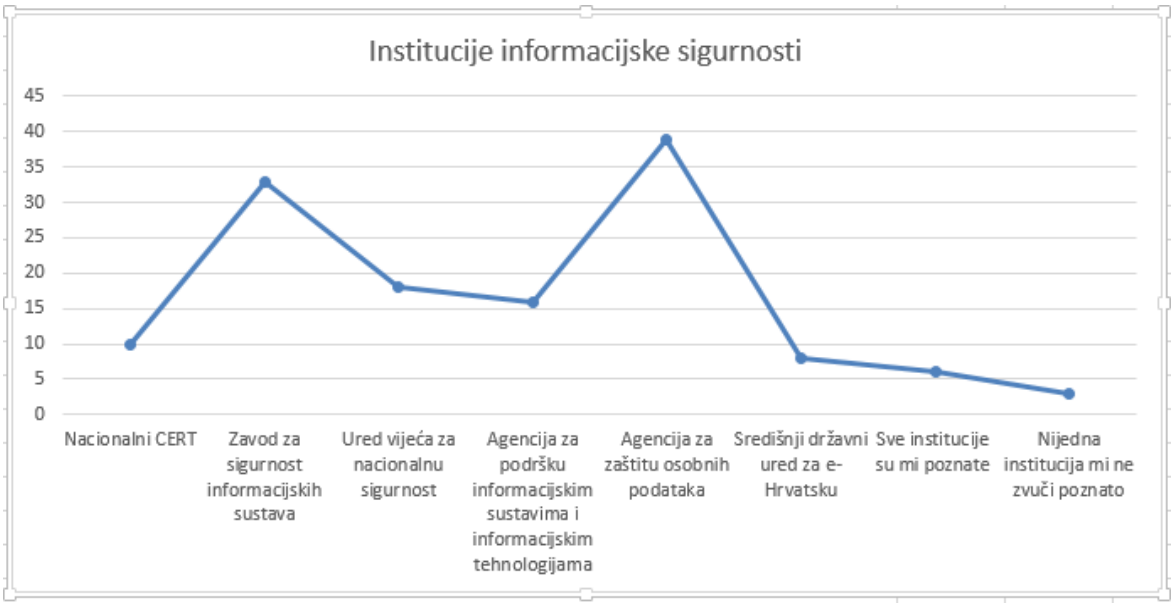


Izvor: izradila studentica prema rezultatima vlastite ankete

Kao što se vidi iz grafikona najviše ispitanika su "obični" zaposlenici, od 50 ispitanih 28 je zaposlenika odgovaralo na anketu, prate ih vlasnici s 8, te voditelji poslovanja s 6 ispitanika. Od 50 ispitanih bilo je 4 direktora, i po 2 asistenta direktora te menadžera. S obzirom na ovaj sastav ispitanika, dalje u radu će se najviše analizirati mišljenja zaposlenika.

Na grafikonima 2. i 3. prikazani su rezultati ankete s obzirom na informiranost ispitanika o zakonima, institucijama te standardima tj. normama koje se koriste kako bi se štitila sigurnost informacijskih sustava.

Grafikon 2. Institucije informacijske sigurnosti

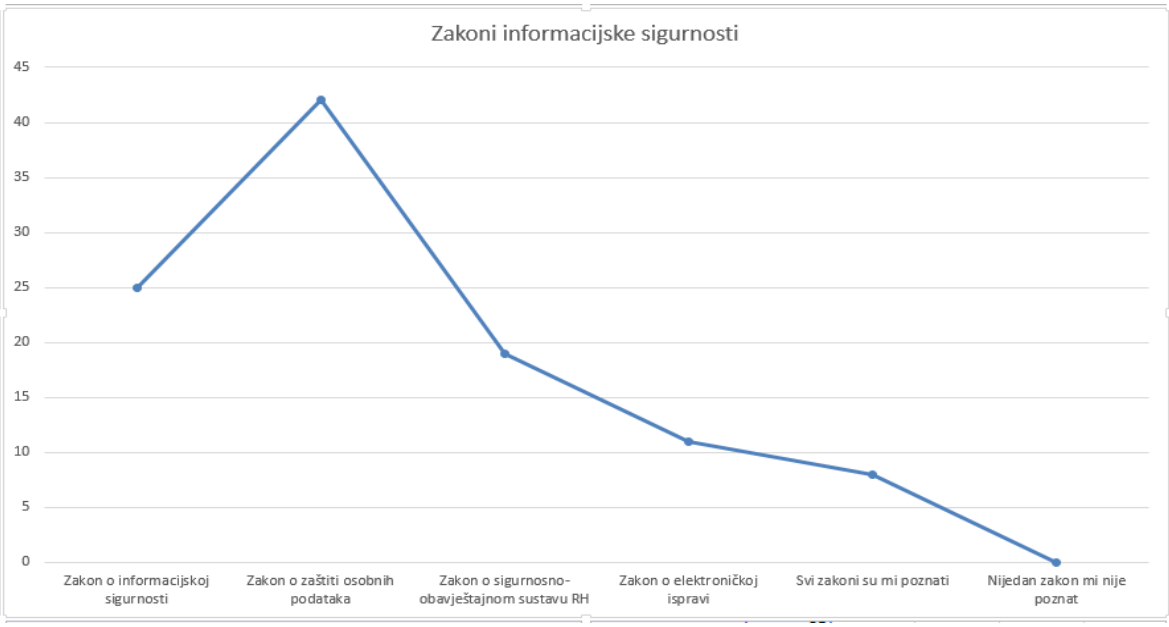


Izvor: izradila studentica prema rezultatima vlastite ankete

S obzirom da su na ovo pitanje ispitanici mogli odabrati više ponuđenih odgovora stanje u državi nije baš na očekivanoj razini informiranosti o zaštiti informacijskih sustava. Samo je 12% ispitanika označilo da prepoznaje po imenu ili zna nešto u vezi uloge ovih institucija, dok troje od 50 ispitanika odnosno malih 0,06% nikad nije ni čulo za niti jedan od ponuđenih odgovora. Najviše ispitanika, čak 39 od 50, prepoznalo je Agenciju za zaštitu osobnih podataka kao jednu od "najpoznatijih" institucija koje se bave informacijskom sigurnošću. Nacionalni CERT prepoznalo je 10 ispitanika, Zavod za sigurnost informacijskih sustava 33 ispitanika, Ured vijeća za nacionalnu sigurnost 18 ispitanika, Agenciju za podršku informacijskim sustavima i informacijskim tehnologijama 16 ispitanika te Središnji državni ured za e-Hrvatsku ispitanika.

Što se tiče zakona vezanih uz sigurnost informacijskih sustava, nešto je drugačija situacija kada je riječ o informiranosti ispitanika. Čak 16% ispitanika odabralo je odgovor da prepoznaju po imenu ili znaju nešto o svim zakonima koji su bili ponuđeni u odgovorima. Niti jedan ispitanik nije označio ponuđen odgovor kako ne prepoznaje niti jedan zakon o sigurnosti informacijskih sustava što je vrlo pohvalno. Gotovo svi ispitanici označili su Zakon o zaštiti osobnih podataka kao zakon za kojeg su čuli ili znaju nešto o njemu. Zakon o informacijskoj sigurnosti te Zakon o sigurnosno-obavještajnom sustavu RH prepoznalo je otprilike pola ispitanika, dok za Zakon o elektroničkoj ispravi zna 11 od 50 ispitanika.

Grafikon 3. Zakoni informacijske sigurnosti



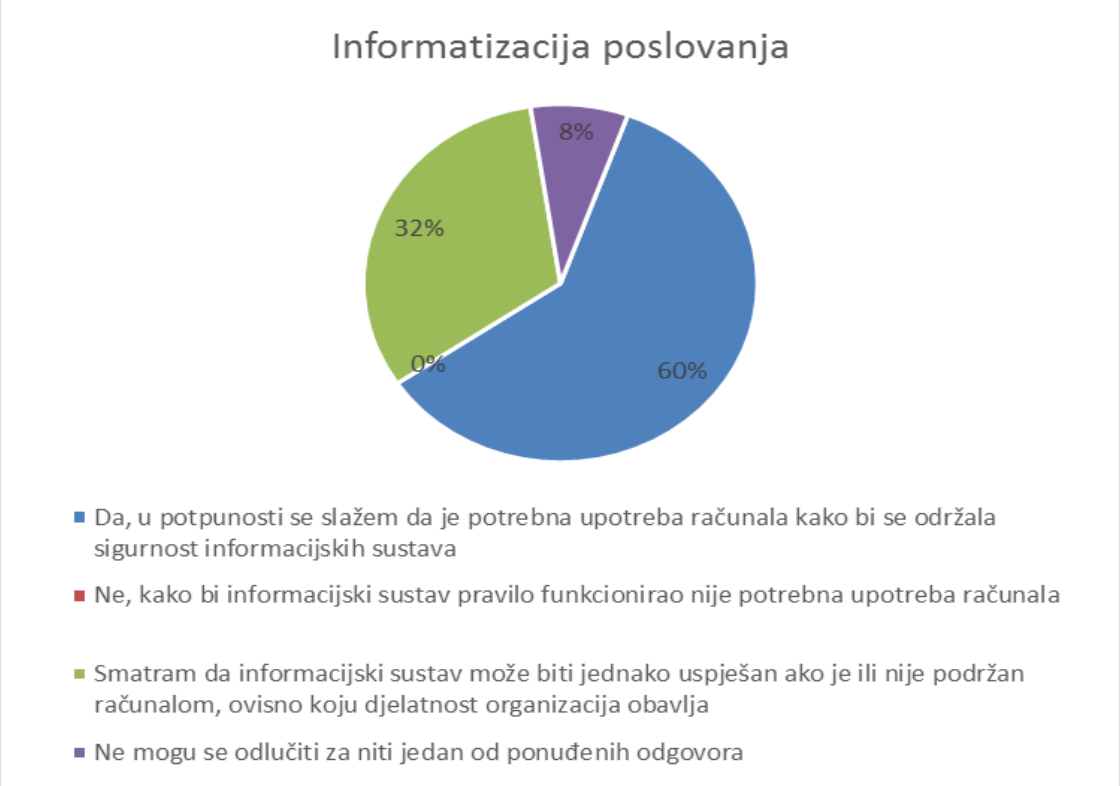
Izvor: izradila studentica prema rezultatima vlastite ankete

Institucije i zakoni Republike Hrvatske koji se brinu o sigurnosti informacijskih sustava prema rezultatima provedene ankete nisu baš "popularni" među ispitanicima. Još im je manje poznato kako su standardi odnosno norme ISO 27001-Sustav upravljanja informatičkom sigurnošću te ISO 27002-Kodeks postupaka za upravljanje sustava informacijske sigurnosti, zapravo standardi koji su od velike važnosti za sigurnost informacijskih sustava kako na međunarodnoj razini tako i na razini države. Samo 28% ispitanika znalo je tu informaciju dok preostalih 72% ni nezna kako se koriste norme u poslovanju za postizanje određene razine sigurnosti informacija.

Unutar ankete nalazilo se pitanje o informatizaciji poslovanja odnosno smatraju li ispitanici da je za pravilnu zaštitu informacijskih sustava potrebno koristiti računala,

odnosno da li sustav koji je siguran mora koristiti računalo. Na grafikonu 4. prikazani su rezultati prema kojima se vidi da je mišljenje ispitanika kako upravo informatizacija poslovanja doprinosi sigurnosti, odnosno kako sustavi koji su podržani računalom odašilju veću razinu zaštite od onih koji nisu podržani računalom.

Grafikon 4. Informatizacija poslovanja



Izvor: izradila studentica prema rezultatima vlastite ankete

Čak 30 od 50 ispitanika odnosno 60 % odlučilo se za tu opciju kako je potrebno računalo za očuvanje sigurnosti informacijskih sustava, nitko se nije složio s tvrdnjom da nije potrebno računalo u tu svrhu, dok se 32% odnosno njih 16 od 50 odlučilo za tvrdnju da je ovisno o djelatnosti koju organizacija obavlja potrebno ili nije potrebno uključiti rad računala u svrhu očuvanja sigurnosti informacijskih sustava. Četiri od 50 ispitanika nije se moglo odlučiti za niti jedan od ponuđenih odgovora.

Prema mišljenju ispitanika organizacije bi trebale koristiti kombinaciju svih mjera zaštite informacijskih sustava. Svega nekoliko ispitanika odlučilo se za pojedinačnu upotrebu mjera zaštite no 74% ispitanika slaže se kako je upravo kombinacija svih mjera zaštita zaslužna za pravilno očuvanje sigurnosti informacijskih sustava.

Za kraj ispitanici su na postavljenu tvrdnju: "„Sigurnost informacijskih sustava pomaže pri rješavanju određenih problema vezanih uz osiguranje kontinuiteta poslovanja te upravljanje sigurnošću informacija u suvremenim organizacijama." odgovarali sa "da-ne" odnosno slažu li se s tvrdnjom ili ne. Samo 2% odnosno 1 ispitanik od 50 je odabrao negativan odgovor, dok je njih 49 od 50 ili 98% odabralo da se slaže s tvrdnjom i tim odabirom potvrdili kako je u Republici Hrvatskoj ipak svjesnost o zaštiti informacija i njihovoj upotrebi u poslovanju na zavidnoj razini.

6. ZAKLJUČAK

Svaki uspješan poslovni sustav sastoji se od niza informacija potrebnih za poslovanje, a za pravilnu upotrebu tih informacija unutar poslovnog sustava postoji informacijski sustav. Informacijski sustav brine o tome da se podaci pretvore u informacije, obrađuju se te interpretiraju na način koji je potreban za poslovanje. Funkcija odnosno cilj kvalitetno izgrađenih informacijskih sustava je osigurati rast i razvoj, produktivnost te učinkovitost organizacije.

Kada se spomene informacijski sustav, većini će prva asocijacija biti računalo, odnosno rad na računalu. U stvarnosti postoje informacijski sustavi koji uopće nisu podržani računalom, a funkcioniraju bez poteškoća. Ono što je važno na spomen informacijskih sustava je zapravo uloga odnosno prikupljanje, obrada, čuvanje i raspodjela podataka neovisno o radu računala. U suvremeno doba iako nije nužno gotovo svaka organizacija ima informacijske sustave podržane računalima. Kako bi se dokazalo da računalo nije nužno za funkcioniranje informacijskih sustava dovoljno je osvrnuti se u prošlost kada su se podaci obrađivali ručno, mehanički ili elektromehanički, a tek izumom ENIAC-a polovicom dvadesetog stoljeća počinju se koristiti računala u te svrhe. Informatizaciji poslovanja u mnogočemu svoj doprinos dali su pad cijena hardvera, mogućnost prilagodbe softvera po mjeri, sve veća količina podataka koje je potrebno obraditi te informacijska zrelost ljudskih resursa.

U današnje vrijeme postoji širok spektar vrsta informacijskih sustava, najgrublja podjela je na informacijske sustave prema konceptualnom ustrojstvu poslovodstva, prema namjeni ili prema modelu poslovnih funkcija u poslovnom svijetu. Samim time što je toliko podjela, a još više podjela unutar tih glavnih vidi se važnost funkcioniranja tog djela u poslovnom sustavu. Odabirom pravog I odgovarajućeg informacijskog sustava za poslovanje bitno utječe na cjelokupno poslovanje neke organizacije.

Sigurnost informacijskih sustava oduvijek je bila važna kako bi neka organizacija uspješno poslovala. Samom modernizacijom i informatizacijom poslovanja rizik sigurnosti informacijskih sustava se povećava. Upravo umrežavanje računala i dislociranost grana poslovanja neke organizacije dovodi do potrebe za većom zaštitom povjerljivih informacija. Kada informacije nisu štićene na pravilan način vrlo je vjerojatno da to može ugroziti konkurentnost organizacije i predstaviti istu organizaciju kao neuspješnom.

S obzirom da sigurnost nije nešto što je konačni proizvod ili stanje, već process logično je da i sigurnost informacijskih sustava predstavlja konstantne radnje i cjelokupan proces zaštite. Nije dovoljno samo odrediti koji informacijski sustavi odgovaraju poslovanju, protrebno je konstantno provjeravati rad sustava kako bi se održala prihvatljiva razina rizika koja prijeti svakom informacijskom sustavu pa tako i poslovnom sustavu u cjelini. Postoji čitav niz dijelova nekog

sustava ili organizacije koje je potrebno štiti, a informacijska sigurnost brine se za tri osnovna aspekta očuvanja povjerljivosti, integriteta te dostupnosti informacija. Kroz ta tri aspekta i pravilnu zaštitu istih moguće je dovesti do napretka poslovanja neke organizacije.

Velik je broj raznih procedura, zakona, pravila, metoda i mjera zaštite informacija u Hrvatskoj i upravo zbog te gomile „pravila“ teško je snaći se i pravilno postupati. O sigurnosti informacijskih sustava brinu se institucije: Nacionalni CERT, Zavod za sigurnost informacijskih sustava, Ured vijeća za nacionalnu sigurnost, Agencija za podršku informacijskim sustavima i informacijskim tehnologijama, Agencija za zaštitu osobnih podataka te Središnji državni ured za e-Hrvatsku. Osim navedenih institucija, zakoni iz područja informacijske sigurnosti su: Zakon o informacijskoj sigurnosti, Zakon o zaštiti osobnih podataka, Zakon o tajnosti podataka te Zakon o elektroničkoj ispravi. Uz institucije i zakone djeluju i određene norme za zaštitu informacijske sigurnosti, a najpoznatije su: ISO 27001:2005 – Sustav upravljanja informatičkom sigurnošću, te ISO 27002:2013 – Kodeks postupaka za upravljanje informacijskom sigurnošću. Iako u Hrvatskoj postoji toliko puno oblasti koje se bave zaštitom informacijskih sustava bitno je naglasiti da prema provedenoj anketi zaposlenici, vlasnici te ostali korisnici neke organizacije nisu dovoljno upoznati sa zakonskom regulativom Republike Hrvatske koja se tiče sigurnosti informacijskih sustava. Činjenica je da najviše ugroza informacijske sigurnosti čine upravo zaposlenici koji namjerno ili nenamjerno čine postupke kojima informacije protiču na mjesta gdje ne bi trebale i na taj način ugrožava se sigurnost informacijskih sustava. Stoga je potrebno da svi koji su uključeni u rad organizacije poznaju i poštuju zakonsku regulativu vezanu uz tu vrstu sigurnosti kako ne bi ugrozili istu. Kako bi funkcionirala pravilna zaštita informacija jedan od najbitnijih faktora je da su zaposlenici i svi korisnici u organizaciji pravilno educirani o tom problemu.

Budući da su informacije glavni resurs poslovanja i da su one srž svega što neka organizacija posjeduje, upravo pravilnom primjenom metoda zaštite povećava se konkurentnost te uspješnost poslovanja određene organizacije. Kako bi neki informacijski sustav bio pravilno zaštićen potrebno je koristiti kombinaciju mjera zaštite informacijskih sustava. Postoje razne vrste zaštite informacijskih sustava. Hardversko softverske mjere uključuju zakonsku zaštitu softvera pomoću raznih metoda, programske mjere zaštite kao što su kriptiranje i antivirusni programi. Uz hardversko softversku zaštitu podataka i informacija postoje i organizacijsko-administrativna te fizička zaštita podataka. Fizička zaštita podataka uz sve ostale sisteme uključuje zaštitare, alarme te nadzorne kamere, dok se organizacijsko.administrativnom zaštitom smatra zaštita na razini podjela odgovornosti i pristupa određenim informacijama s obzirom na ulogu u organizaciji. Nije dovoljno upotrijebiti primjerice samo fizičku zaštitu ili samo hardversko-softversku zaštitu. Potrebno je pravilnom kombinacijom svih mjera zaštite štititi informacije, te je potrebno implementirati u rad

organizacije sve zakone i ostale procedure i upute kojima se može očuvati sigurnost informacijskih sustava.

Ono što čini bitan vid poslovanja je pravilno se odlučiti o mjerama zaštite koje će se koristiti, ovisno o organizaciji i djelatnosti s kojom se određena organizacija bavi važno je provesti pravilne zaštite. Sigurnost informacijskih sustava ne uključuje samo pohranu povjerljivih podataka na posebno mjesto, već je potrebno štititi same objekte, opremu prostore, pa sve do programa i dokumenata koji sadrže informacije. Razlog kompleksnosti zaštite informacijske sigurnosti nalazi se upravo na toj razini što je sigurnost informacijskih sustava jako širok pojam te ga je potrebno sagledati kao cjelinu, a ne obraćati pažnju na samo neke određene dijelove.

Kada se informacijski sustav shvati kao jedna velika cjelina razgranata na razna područja, i kada se poštuju zakoni, pravila, procedure i upute iz te oblasti tek tada se može govoriti da je neki informacijski sustav siguran. Međutim upravo zbog razgranatosti i kompleksnosti ove tematike vrlo je teško pratiti u potpunosti sigurnost informacijskih sustava, jer su oni u mnogo čemu ranjivi pa je potrebno kontinuirano provjeravati i čuvati se prijetnji koje današnjim razvojem tehnologije i programa sve više postaju otvoreni za nove prijetnje.

Moderno informacijsko društvo postavlja nove uvjete potrebne za očuvanje sigurnosti. S obzirom da je u Republici Hrvatskoj i više nego dovoljno zakona, instirucija, standarda, pravila i procedura zaštite informacijskih sustava to znači da je svjesnost o važnosti ovog područja naše države na visokoj razini. Ono što bi trebalo promijeniti je to da bi zaposlenici trebali biti bolje educirani o važnosti očuvanja sigurnosti informacija. Informacija u pravo vrijeme i na pravom mjestu dovodi do uspješnog poslovanja, a ako povjerljiva informacija „iscuri“ na neželjena mjesta propada ugled neke organizacije, efikasnost i konkurentnost iste.

Ovim zaključcima i kompletnim radom dokazana je hipoteza da u Republici Hrvatskoj postoji veliki broj zakona, procedura, pravila te ostale regulative kojima se upravlja informacijskom sigurnošću, ali su zaposlenici i dalje nedovoljno educirani, pa se informacije ne štite na prikladan način.

LITERATURA

KNJIGE:

1. Antoliš, K.,et al, Sigurnost informacijskih sustava : priručnik. Zagreb : Algebra, 2010.
2. Dragičević, D., Kompjutorski kriminalitet i informacijski sustavi. Zagreb : Informator, 1999.
3. Hadjina, N., Zaštita informacijskih susava. Zagreb: FER, 2009.
4. Klasić, K., Klarin, K., Informacijski sustavi : načela i praksa. Zagreb : Intus informatika, 2009.,
5. Panian, Ž. Kontrola i revizija informacijskih sustava. Zagreb : Sinergija - nakladništvo, 2001.
6. Pavlić, M. Informacijski sustavi. Zagreb: Školska knjiga, 2011.
7. Šehanović, J., Hutinski, Ž., Žugaj, M., Informatika za ekonomiste, Tiskara Varteks, 2002.

ČLANCI:

8. Bogati, J., Norme informacijske sigurnosti ISO/IEC 27K ,Praktični menadžment, Vol. II, br. 3, str. 112-117, 2011 godina
9. Davis, G.B., Olson, M.H., Management Information Systems: Conceptual Foundations, Structura andDevelopment, McGraw- Hill, New York, SAD, 1985., str. 200-202
10. Klasić, K. Zaštita informacijskih sustava u poslovnoj praksi.// SIGURNOST, Vol.49 No.1 Travanj 2007.
11. Prelog, N. Informacijski sustavi za zaštitu i poboljšanje okoliša. //Treći program Hrvatskog radija, 1990, 28, str. [176]-184.

INTERNET:

12. http://autopoiesis.foi.hr/wiki.php?name=KM++Tim+55&parent=NULL&page=Obrada%20podataka, 30.07.2014.
13. http://www.referenceforbusiness.com/management/Comp-De/Data-Processing-and-Data-Management.html, 30.07.2014.

14. http://ossunist.files.wordpress.com/2013/06/informacijski-sustavi-skripta.pdf, 30.07.2014.
15. http://www.unizd.hr/portals/1/primjena_rac/brodostrojarstvo/predavanje_1.pdf, 30.07.2014.
16. http://www.zbrdazdola.com/infobible/infobible/razvoj_racunala_kroz_povijest.htm, 30.07.2014.
17. http://www.columbia.edu/cu/computinghistory/census-tabulator.html, 10.05.2014.
18. http://www.linfo.org/eniac.html, 30.07.2014.
19. http://www.promeng.eu/downloads/training-materials/ebooks/business-information-systems.pdf, 30.07.2014.
20. http://ossunist.files.wordpress.com/2013/06/informacijski-sustavi-skripta.pdf, 30.07.2014.
21. http://hr.wikipedia.org/wiki/Informacijski_sustavi, 30.07.2014.
22. http://ossunist.files.wordpress.com/2013/06/informacijski-sustavi-skripta.pdf, 30.07.2014.
23. http://www.techopedia.com/definition/25830/cia-triad-of-information-security, 30.07.2014.
24. http://www.cert.hr/onama, 05.06.2014.
25. http://hr.wikipedia.org/wiki/Zavod_za_sigurnost_informacijskih_sustava, 05.06.2014.
26. http://www.uvns.hr/default.aspx?id=109, 05.06.2014.
27. http://www.uvns.hr/default.aspx?id=43,
28. http://hujak.hr/clan-apis-it/, 05.06.2014.
29. http://sigurnost.lss.hr/images/dokumenti/lss-pubdoc-2010-10-003.pdf, 05.06.2014.
30. http://hr.wikipedia.org/wiki/Sredi%C5%A1nji_dr%C5%BEavni_ured_za_e-Hrvatsku, 05.06.2014.
31. http://narodne-novine.nn.hr/clanci/sluzbeni/298919.html, 06.06.2014.
32. http://narodne-novine.nn.hr/clanci/sluzbeni/305952.html, 06.06.2014.
33. http://www.propisi.hr/print.php?id=5045, 06.06.2014.
34. http://www.zakon.hr/z/272/Zakon-o-elektroni%C4%8Dkoj-ispravi, 09.07.2014.
35. http://www.poslovniforum.com/nnhr/2005-12-150-2898.html, 30.07.2014.
36. http://iso-17799.safemode.org/, 30.07.2014.
37. http://os2.zemris.fer.hr/ISMS/2008_poljak/Poljak_Ivan_diplomski_rad_1716.pdf, 30.07.2014.
38. http://www.iso27001standard.com/hr/sto-je-iso-27001, 30.07.2014.
39. http://security.foi.hr/wiki/index.php/ISO_27002_-_Norma_i_Sukladnost, 02.08.2014.
40. http://blog.iso27001standard.com/2013/02/11/main-changes-in-the-new-iso-27002-2013-draft-version/, 31.07.2014
41. http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2004-04-71.pdf, 16.08.2014.

42. http://www.itvestak.org.rs/ziteh_04/radovi/ziteh-28.pdf, 16.08.2014.
43. http://www.digitconsulting.rs/index.php/licenciranje-microsoft/licenciranje/sofverska-licenca.html, 16.08.2014.
44. http://www.am.unze.ba/rg/2007/zastita%20digitalnih%20podataka/HTML/dongle.html, 16.08.2014.
45. http://www.am.unze.ba/rg/2007/zastita%20digitalnih%20podataka/HTML/instalacijski%20mediji.html, 16.08.2014.
46. http://security.foi.hr/wiki/index.php/Za%C5%A1tita_programskih_proizvoda, 16.08.2014.
47. http://www.am.unze.ba/rg/2007/zastita%20digitalnih%20podataka/HTML/registracijske%20sifre.html, 16.08.2014.
48. http://www.unizd.hr/Portals/1/Primjena_rac/Poseban_program/Predavanja/sigurnost_predavanje.pdf, 24.08.2014.
49. http://hr.wikipedia.org/wiki/Kriptografija, 20.08.2014.
50. http://hr.wikipedia.org/wiki/Ra%C4%8Dunalni_virus#cite_ref-virusi_2-0, 20.08.2014.
51. http://sh.wikipedia.org/wiki/Spyware, 20.08.2014.
52. http://www.smart.rs/Start/Usluge/Impl/ITbezbednost/Stranice/Firewall.aspx, 20.08.2014.
53. http://es.scribd.com/doc/17094401/50/Kontrola-pristupa, 19.08.2014.
54. http://os2.zemris.fer.hr/ISMS/2008_kovacevic/primjerSP_2.html, 19.08.2014.
55. https://www.fer.unizg.hr/poslijediplomski/specijalisticki_studij/informacijska_sigurnost, 19.08.2014.
56. http://www.scribd.com/doc/17094401/13/suradnja-izme%C4%91u-organizacija, 19.08.2014
57. http://www.scribd.com/doc/17094401/47/Upravljanje-mre%C5%BEom, 19.08.2014.
58. http://os2.zemris.fer.hr/ISMS/2008_kovacevic/primjerSP_2.html, 19.08.2014.
59. http://www.moj-posao.net/Vijest/60807/Outsourcing-sto-je-i-zasto-se-koristi/, 20.08.2014.
60. http://www.scribd.com/doc/17094401/Sigurnost-informacijskih-sustava, 20.08.2014.
61. http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-06-304.pdf, 30.08.2014.
62. http://security.lss.hr/arhiva-dokumenata/fizicka-sigurnost-informacijskog-sustava.html, 31.08.2014.

63. http://en.wikipedia.org/wiki/Crime_prevention_through_environmental_design, 31.08.2014.
64. http://www.alarmautomatika.com/idea-project/document/09028-rjesenja-kontrole-pristupa-i-evidencije-radnog-vremena.pdf, 31.08.2014.
65. http://books.google.hr/books?id=hbQIAAAAQBAJ&pg=SA1-PA19&lpg=SA1-PA19&dq=eps+electronic+physical+security&source=bl&ots=aRKzXXSs9f&sig=qNg6b738bpu58WYyCfR63fMBLlY&hl=hr&sa=X&ei=FZEEVLCIB4fmyQPT2ILgBw&ved=0CBoQ6AEwAA#v=onepage&q=eps%20electronic%20physical%20security&f=false
66. http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-06-304.pdf, 31.08.2014.
67. http://www.aam-mihalinec.hr/kontrola-pristupa.php, 31.08.2014
68. http://www.condorsecuritybih.com/#!noviteti-najnovije-opreme-na-titu/chbg, 31.08.2014.

POPIS TABLICA

POPIS SLIKA

POPIS GRAFIKONA